nit I : Information Security Overview, Risk Analysis & Secure Design Princip

LLABUS Weightage : 15 Marks

formation Security Overview : The Importance of Information Protection, The volution of Information Security, Justifying Security Investment, Security Methodology, ow to Build a Security Program, The Impossible Job, The Weakest Link, Strategy and actics, Business Processes vs. Technical Controls.

isk Analysis : Threat Definition, Types of Attacks, Risk Analysis.

ecure Design Principles : The CIA Triad and Other Models, Defense Models, Zones of Trust, Best Practices for Network Defense.

opics :

1 **Information Security Overview**
2 **Risk Analysis**
3 **Secure Design Principles**

protect the Information?

Information is an important asset. Anywhere information is often one of the most important assets.

Organizations broadly classifies information in various ways :

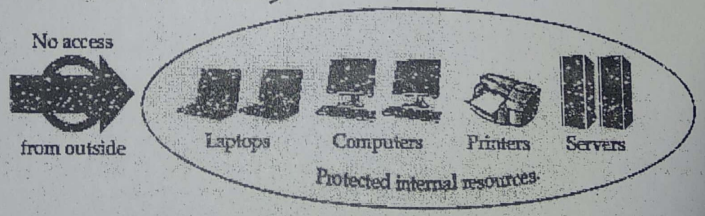
1. Labeling (to specify how it should be handled)
2. Distribution (who gets to see it)
3. Duplication (how replicas are made and handled)
4. Release (how it is released)
5. Storage (where it is stored)
6. Encryption (plain text to cipher text)
7. Disposal (whether it is temporary or permanent deleted)
8. Methods of transmission (Mail, fax, etc).

Companies may have **confidential information**, such as research and development plans, manufacturing processes, strategic corporate information, product roadmaps, process descriptions, customer lists and contact information, financial forecasts, and earnings announcements that is intended for internal use on a need-to-know basis. Loss or theft of confidential information could reduce the company's competitive advantage, or cause damage to the company. This type of information is available to external audiences only for business-related purposes and only after entering a nondisclosure agreement (NDA).

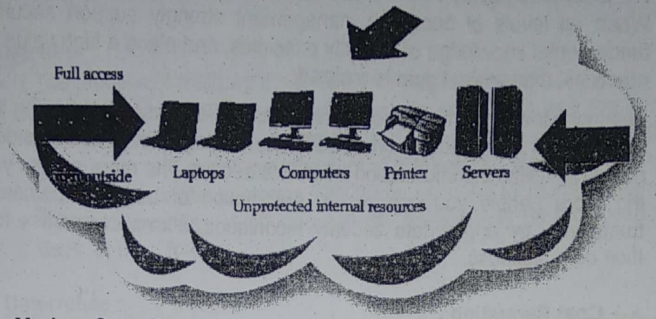
Specialized information or **secret information** may include trade secrets, such as formulas, production details, and other intellectual property, proprietary methodologies and practices that describe how services are provided, research plans, electronic codes, passwords, and encryption keys. If disclosed, this type of information may severely damage the company's competitive advantage. It is usually restricted to only a few people or departments within a company and is rarely disclosed outside the company.

Q.2 How the information security Evolved?

Ans.: In the early days of networking, individual computers were connected together only in academic and government environments. So the networking technologies that were developed were specific to academic and government environments. Originally, the academic security model was "open" and the government security model was "closed." The government was mainly concerned with blocking access to computers, restricting internal access to confidential data, and preventing interception of data.

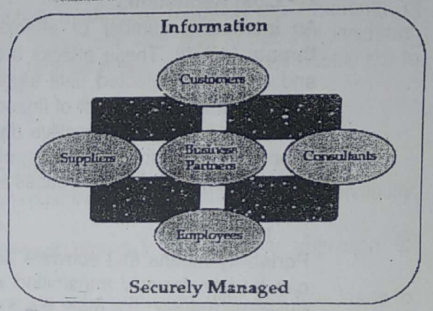


In the academic world, the goal was to share information openly, so security controls were limited to accounting functions in order to charge money for the use of computer time. There is need to combine both the models as there is plenty of room in between these two extremes.



Modern Security :

Modern security products are now designed to balance the needs of business on the Internet while protecting against today's sophisticated threats.



Four classes of Threats :

- **Interception :** Unauthorized party has gain access to an asset. The outside party can be person, a program or a computing system.
- **Interruption :** An asset of the system becomes lost, unavailable, or unusable e.g., Malicious destruction of a hardware device, erasure of a program or data file, or malfunction of an operating system file manager so that it cannot find a particular disk file.
- **Modification :** Accessing and tamper with asset e.g., modifying program so that it perform additional computing.
- **Fabrication :** An unauthorized party create a fabrication of counterfeit objects on a computing system.

Q.3 Write a short note on Security Investment.

Ans.: Initially there was a fear, uncertainty, and doubt. Without really measuring anything organization were in fuzzy state into spending money. So, return on investment (ROI) was used as an attempt to market security as an investment that "pays for itself." This was the standard approach to justifying information technology budgets, but it never translated well to security.

Further "insurance analogy" was developed as an alternative to value-based security justifications. They spend this money for peace of mind, knowing that they will be covered in the event of a problem.

Specific benefits of a strong security program are business agility, cost reduction, and portability :

- **Business Agility :**

When all levels of company management strongly support security, have a fundamental knowledge of security principles, and place a high value on security practices, the greatest gain is realized.

Security allows information to be used more effectively in advancing the goals of organization because that organization can safely allow more outside groups of people to utilize the information when it is secure. The more access you provide, the more people you can reach. Automation of business processes, made trustworthy by appropriate security techniques, allows companies to focus on their core business.

- **Cost Reduction :**

An increasing number of attacks are categorized as **advanced persistent threats** (APTs). These attacks are designed to deploy malware into a network and remain undetected until triggered for some malicious purpose. Often, the goal of the attacks is theft of financial information or intellectual property. Loss of service or leakage of sensitive data can result in fines, increased fees, and an overall decrease in corporate reputation and stock price. Strong security reduces loss of information and increases service availability and confidentiality.

- **Portability :**

Portability means that software and data can be used on multiple platforms or can be transferred / transmitted within an organization, to a customer, or to a business partner. To meet the demands of today's businesses and consumers, architectures and networks need to be designed with security controls baked in as part of the development process. Clearly, this level of broad access to information resources requires a well-thought-out and properly deployed security program.

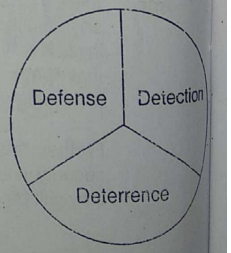
Q.4 What are the 3D's of security?

Ans.:

- The field of **security** is concerned with protecting assets in general.
- **Information security** is concerned with protecting information.
- **Network security** is concerned with protecting data, hardware, and software on a computer network.

3D's of security : The basic assumptions of security are as follows :

- We want to protect our assets.
- There are threats to our assets.
- We want to mitigate those threats.



Defense :

- The process of proactively be protective to withstand the different attacks is said to be a defensive mechanism.

- Defensive controls on the network can include access control devices such as *stateful firewalls, network access control* spam and malware filtering, *web content filtering*, etc.
- These controls provide protection from software vulnerabilities, bugs, attack scripts, ethical and policy violations, accidental data damage.

Detect :

- The process of realizing the threat is known as detection.
- Detective controls on the network include audit trails and log files, system and network intrusion detection and prevention systems and security information and event management (SIEM) alerts, reports, and dashboards. A security operations center (SOC) can be used to monitor these controls. Without adequate detection, a security breach may go unnoticed for hours, days, or even forever.

Deterrence :

- It is considered to be an effective method of reducing the frequency of security compromises, and thereby the total loss due to security incidents. With the use of deterrent controls such as these, attackers may decide not to cause damage.

Q.5 How to Build a Security Program?

Ans.: There are many components that go into the building of a security program :

- **Authority :** The security program must include the right level of responsibility and authorization to be effective.
- **Framework :** A security framework provides a defensible approach to building the program.
- **Assessment :** Assessing what needs to be protected, why, and how leads to a strategy for improving the security posture.
- **Planning :** Planning produces priorities and timelines for security initiatives.
- **Action :** The actions of the security team produce the desired results based on the plans.
- **Maintenance :** The end stage of the parts of the security program that have reached maturity is to maintain them.

The Impossible Job

The job of the attacker is always easier than the job of the defender. The attacker needs only to find one weakness, while the defender must try to cover all possible vulnerabilities Every defender performs a risk assessment by choosing which threats to defend against, which to insure against, and which to ignore.

Q.6 Write a short note on weakest link.

Ans.: A security infrastructure will drive an attacker to the weakest link. For example, a potential burglar who is trying to break into a house may start with the front door. If the front door lock is too difficult to pick, the burglar may try side doors, back doors, and other entrances. If the burglar can't get through any of those, he may try to open a window. If they're all locked, he may try to break one. If the windows are unbreakable or barred, he may try to find other weaknesses. If the doors, windows, roof, and basement are all impenetrable, a determined burglar may try to cut a hole

in the wall with a chainsaw. All security controls should complement each other, and each should be equally as strong as the others. This principle is called *equivalent security* or *transitive security*. One more example is storing credit card details at different location and securing all those location is most important.

In any case, weak points in the security infrastructure should be avoided whenever possible. In situations where weak points are necessary due to business requirements, detective and deterrent security controls should focus on the areas where defensive weak points exist.

Strategy and Tactics :

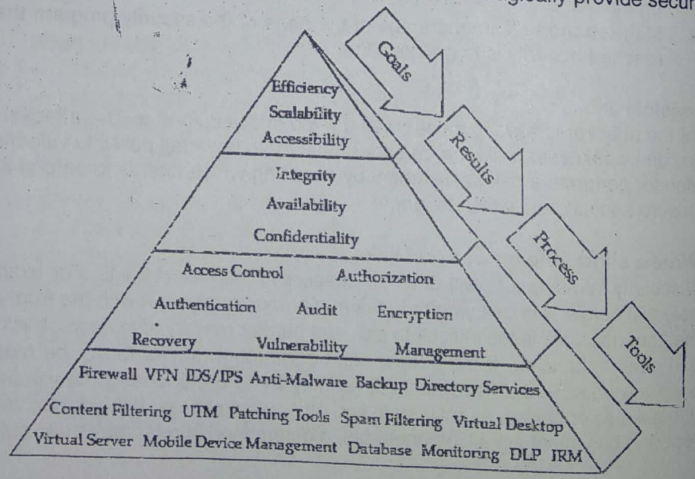
In any case, weak points in the security infrastructure should be avoided whenever possible. In situations where weak points are necessary due to business requirements, detective and deterrent security controls should focus on the areas where defensive weak points exist.

Strategic planning can proceed on weekly, monthly, quarterly, and yearly bases, and should be considered an ongoing endeavor. Often there is an immediate need to secure a part of the network infrastructure, and time is not on the side of the strategic planner. In these cases, a tactical solution can be put in place temporarily to allow appropriate time for planning a longer-term solution.

Q.7 What are different business processes and technical controls to facilitate security?

Ans.: Security threats and exposures are complex and constantly evolving. Security technologies need to be selected on the basis of business context, so they are targeted toward specifically identified risks with clear objectives.

Purchasing a database does not solve the problem of how to manage customer data. Customer data management is a business process that can be facilitated by a database. Likewise, buying a firewall doesn't magically provide security.



In the context of network security, business objectives, priorities, and processes determine the choice of tools, and the tools are used to facilitate the business processes.

Make these assumptions when considering security:

- You can never be 100 percent secure.
- You can, however, manage the risk to your assets.
- You have many tools to choose from to manage risk. Used properly, these tools can help you achieve your risk management objectives.

Important Definition :

- **Threat :** An action or event that might prejudice security. A threat is a potential violation of security.
- **Vulnerability :** Existence of a weakness, design, or implementation error that can lead to an unexpected, undesirable event compromising the security of the system.
- **Target of Evaluation :** An IT system, product, or component that is identified/ subjected as requiring security evaluation.
- **Attack :** An assault on system security that derives from an intelligent threat. An attack is any *action* that violates security.
- **Exploit :** A defined way to breach the security of an IT system through vulnerability.

1.2 RISK ANALYSIS

Q.1 Write a short note on threats in security.
OR
Explain basic threats in security.

Ans.: A computer-based system has three separate but valuable components: **hardware, software, and data.** Each of these assets offers value to different members of the community affected by the system. To analyze security, we can brainstorm about the ways in which the system or its information can experience some kind of loss or harm. For example, we can identify data whose format or contents should be protected in some way. We want our security system to make sure that no data are disclosed to unauthorized parties. Neither do we want the data to be modified in illegitimate ways. At the same time, we want to ensure that legitimate users have access to the data. In this way, we can identify weaknesses in the system, A **vulnerability** is a weakness in the security system, for example, in procedures, design, or implementation, that might be exploited to cause loss or harm. For instance, a particular system may be vulnerable to unauthorized data manipulation because the system does not verify a user's identity before allowing data access.

A threat to a computing system is a set of circumstances that has the potential to cause loss or harm. To see the difference between a threat and a vulnerability, consider the illustration in Figure below. Here, a wall is holding water back. The water to the left of the wall is a threat to the man on the right of the wall: the water could rise, overflowing onto the man, or it could stay beneath the height of the wall, causing it to collapse. So the threat of harm is the potential for the man

to get wet, get hurt, or drown. For now, the wall is intact, so the threat to the man is unrealized.

However, we can see a small crack in the wall—a vulnerability that threatens the man's security. If the water rises to or beyond the level of the crack, it will exploit the vulnerability and harm the man.

There are many threats to a computer system, including human-initiated and computer-initiated ones. We have all experienced the results of inadvertent human errors, hardware design flaws, and software failures. But natural disasters are threats, too; they can bring a system down when the computer room is flooded or the data center collapses from an earthquake, for example.

A human who exploits a vulnerability perpetrates an attack on the system. An attack can also be launched by another system, as when one system sends an overwhelming set of messages to another, virtually shutting down the second system's ability to function.

How do we address these problems? We use a **control** as a protective measure. That is, a control is an action, device, procedure, or technique that removes or reduces a vulnerability. The man is placing his finger in the hole, controlling the threat of water leaks until he finds a more permanent solution to the problem/In general, we can describe the relationship among threats, controls, and vulnerabilities in this way:

- **A threat is blocked by control of a vulnerability :**

To devise controls, we must know as much about threats as possible. We can view any threat as being one of four kinds: interception, interruption, modification, and fabrication. Each threat exploits vulnerabilities of the assets in computing systems; the threats are illustrated in figure 3.

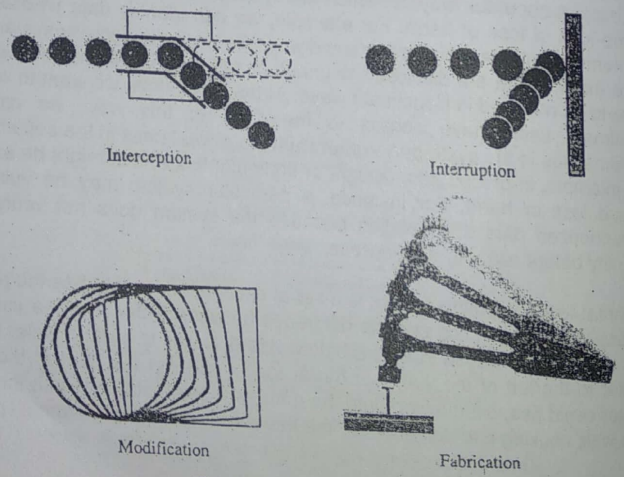


Fig. : System security threats.

- **An interception** means that some unauthorized party has gained access to an asset. The outside party can be a person, a program, or a computing system. Examples of this type of failure are illicit copying of program or data files, or wiretapping to obtain data in a network. Although a loss may be discovered fairly quickly, a silent interceptor may leave no traces by which the interception can be readily detected.

- **In** an **interruption,** an asset of the system becomes lost, unavailable, or unusable. An example is malicious destruction of a hardware device, erasure of a program or data file, or malfunction of an operating system file manager so that it cannot find a particular disk file.

- If an unauthorized party not only accesses but tampers with an asset, the threat is a **modification.** For example, someone might change the values in a database, alter a program so that it performs an additional computation, or modify data being transmitted electronically. It is even possible to modify hardware. Some cases of modification can be detected with simple measures, but other, more subtle, changes may be almost impossible to detect.

- Finally, an unauthorized party might create a **fabrication** of counterfeit objects on a computing system. The intruder may insert spurious transactions to a network communication system or add records to an existing database. Sometimes these additions can be detected as forgeries, but if skillfully done, they are virtually indistinguishable from the real thing.

These four classes of threats—interception, interruption, modification, and fabrication—describe the kinds of problems we might encounter.

Threat Vectors :
A threat vector is a term used to describe where a threat originates and the path it takes to reach a target. An example of a threat vector is an e-mail message sent from outside the organization to an inside employee, containing an irrelevant subject line along with an executable attachment that happens to be a Trojan program, which will compromise the recipient's computer if opened.

Q.2 What are the different defense models?

Ans.: An attack is an information security threat that involves an attempt to obtain, alter, destroy, remove, implant or reveal information without authorized access or permission. It happens to both individuals and organizations.

Types of Attacks :
"Passive" when a network intruder intercepts data traveling through the network, and "Active" in which an intruder initiates commands to disrupt the network's normal operation.

- **Passive attack :** Here are some examples of passive attack:

(a) Traffic analysis : In the traffic analysis attack, an attacker tries to sense the communication path between the sender and receiver. An attacker can found the amount of data which is travel from the route of sender and receiver. There is no modification in data by the traffic analysis.

(b) Eavesdropping : This is a passive attack, which occurred in the mobile ad-hoc network. The main aim of this attack is to find out some secret or confidential information from communication. This secrete information may be privet or public key of sender or receiver or any secrete data.

(c) Monitoring : In this attack in which attacker can read the confidential data, but he cannot edit the data or cannot modify the data.

Active attack : Here are some examples of active attacks :

(a) Spoofing : When a malicious node miss-present his identity, so that the sender change the topology.

(b) Modification : When malicious node performs some modification in the routing route, so that sender sends the message through the long route. This attack cause communication delay occurred between sender and receiver.

(c) Wormhole : This attack is also called the tunneling attack. In this attack an attacker receives a packet at one point and tunnels it to another malicious node in the network. So that a beginner assumes that he found the shortest path in the network.

(d) Fabrication : A malicious node generates the false routing message. This means it generate the incorrect information about the route between devices.

(e) Denial of services : In denial of services attack, malicious node sending the message to the node and consume the bandwidth of the network. The main aim of the malicious node is to be busy the network node. If a message from unauthenticated node will come, then receiver will not receive that message because he is busy and beginner has to wait for the receiver response.

(f) Sinkhole : Sinkhole is a service attack that prevents the base station from obtaining complete and correct information. In this attack, a node tries to attract the data to it from his all neighbouring node. Selective modification, forwarding or dropping of data can be done by using this attack.

(g) Sybil : This attack related to the multiple copies of malicious nodes. The Sybil attack can be happen due to malicious node shares its secret key with other malicious nodes. In this way the number of malicious node is increased in the network and the probability of the attack is also increases. If we used the multipath routing, then the possibility of selecting a path malicious node will be increased in the network.

Virus : *"A computer virus is a program that may disturb the normal working of a computer system".* Virus attaches itself to files stored on floppy disks, USBs, email attachments and hard disks. A file containing a virus is called infected file. If this file is copied to a computer, virus is also copied to the computer.

Malware : Malware is short for malicious software. Malware is the name given to any type of software that could harm a computer system, interfere with and gather a user's data, or make the computer perform actions without the owner's knowledge or permission.

Trojan horse : A type of malware that uses malicious code to install software that seems ok, but is hidden to create back doors into a system typically causing loss or theft of data from an external source.

Worm : Unlike a virus, a worm, is a standalone piece of malicious software that replicates itself in order to spread to other computers. It often uses a computer network to spread itself, relying on security flaws on the target system to allow access.

Spyware : Spyware is software that aids in gathering information about a person or organization without their knowledge, they can monitor and log the activity performed on a target system, like log key strokes, or gather credit card and other information.

Adware : Adware is software which can automatically causes pop-up and banner adverts to be displayed in order to generate revenue for its author or publisher. A lot of freeware will use Adware but not always in a malicious way, if it was malicious, it would then be classed as spyware or malware.

Q.3 How Can a Computer be Protected from Viruses?

Ans.:

- Install an anti-virus program and keep it up-to-date and regularly run scans.
- Install an anti-malware program to stop software installing without your knowledge.
- Never download and install software from the Internet unless you are certain it is from a trusted source.
- Don't open e-mail attachments unless you have scanned them first, even a picture can carry a virus.
- Don't trust cracked or hacked software as they often contain malware, Trojans.

RAT (Remote Access Trojan)

A Remote Access Trojan (RAT) is a malware program that includes a **back door** for administrative control over the target computer. RATs are usually downloaded invisibly with a user-requested program -- such as a game -- or sent as an email attachment. Once the host system is compromised, the intruder may use it to distribute RATs to other vulnerable computers and establish a **botnet**.

DOS and DDOS :

A DDoS attack requires an attacker to gain control of a network of online machines in order to carry out an attack. Computers and other machines (such as IoT devices) are infected with **malware**, turning each one into a bot (or zombie). The attacker then has remote control over the group of bots, which is called a **botnet**.

Once a botnet has been established, the attacker is able to direct the machines by sending updated instructions to each bot via a method of remote control. When the **IP address** of a victim is targeted by the botnet, each bot will respond by sending requests to the target, potentially causing the targeted server or network to overflow capacity, resulting in a **denial-of-service** to normal traffic. Because each bot is a legitimate Internet device, separating the attack traffic from normal traffic can be difficult.

Physical Security :

In today's world of interconnectedness, the least popular means of attack is direct physical access, but if an attacker can physically access a computer, it's game over. They literally can do anything, including physically damage the computer, steal passwords, plant keystrokelogging Trojans, and steal data.

Network-Layer Attacks :

- **Packet Sniffing**
- **Sniffer Attack :** A sniffer is an application or device that can read, monitor, and capture network data exchanges and read network packets. If the packets are not encrypted, a sniffer provides a full view of the data inside the packet. Attacker store the incoming and outgoing data into the packet using network sniffer tool. Apart from network sniffer, lots of packet sniffer and packet analysis tools is available which is used to check the sniffed packed.

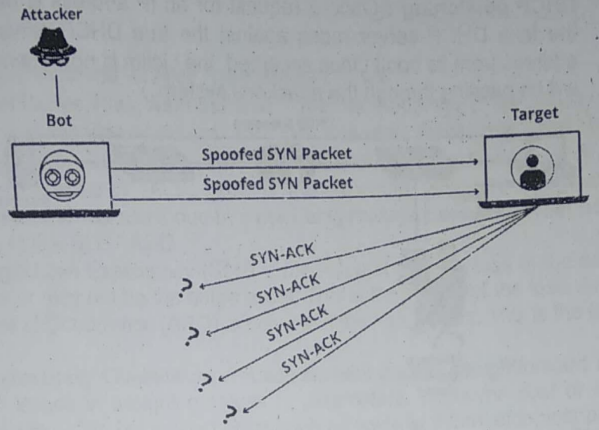
Packet sniffing is a technique of monitoring every packet that crosses the network.

Wiretapping is a process of monitoring the telephone and internet conversations by a third party attackers connect a hardware or software or combination of both to the switch carrying information between two phones or hosts on the internet.

- **Session Hijacking :** It is when a hacker takes control of a user session after the user has successfully authenticated with a server, session hijacking involves an attack identifying the current session ids of a client or server communication and taking over the client.
- **SYN Flooding :** When a client and server establish a normal TCP "three-way handshake," the exchange looks like this :
  1. Client requests connection by sending SYN (synchronize) message to the server.
  2. Server acknowledges by sending SYN-ACK (synchronize-acknowledge) message back to the client.
  3. Client responds with an ACK (acknowledge) message, and the connection is established.

In a SYN flood attack, the attacker sends repeated SYN packets to every port on the targeted server, often using a fake IP address. The server, unaware of the attack, receives multiple, apparently legitimate requests to establish communication. It responds to each attempt with a SYN-ACK packet from each open port.

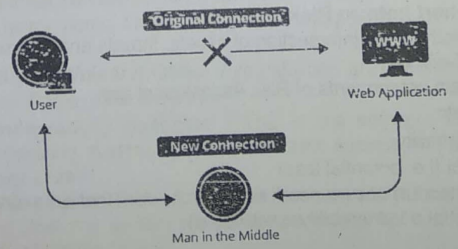
The malicious client either does not send the expected ACK, or—if the IP address is spoofed—never receives the SYN-ACK in the first place. Either way, the server under attack will wait for acknowledgement of its SYN-ACK packet for some time.



Application-Layer Attacks :

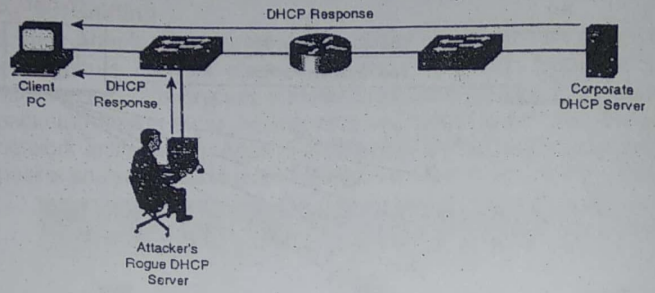
- **Buffer Overflow :** Attackers can exploit a buffer overflow bug by injecting code that is specifically tailored to cause buffer overflow with the initial part of a data set, then writing the rest of the data to the memory address adjacent to the overflowing buffer. The overflow data might contain executable code that allows the attackers to run bigger and more sophisticated programs or grant themselves access to the system.
- **Password Cracking :** Brute-force tools attempt to guess a password by trying all the character combinations listed in an accompanying dictionary.
- **Man in the middle attack :** A man in the middle (MITM) attack is a general term for when a perpetrator positions himself in a conversation between a user and an application—either to eavesdrop or to impersonate one of the parties, making it appear as if a normal exchange of information is underway.

The goal of an attack is to steal personal information, such as login credentials, account details and credit card numbers. Targets are typically the users of financial applications, SaaS businesses, e-commerce sites and other websites where logging in is required.

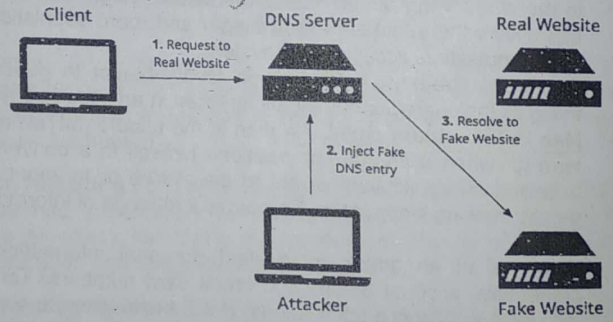


- **ARP Poisionning :** ARP poisoning works by simply responding to Address Resolution Protocol (ARP) requests with the attacker's MAC address.

- **DHCP poisioning :** Once a request for an IP address is heard on the line, the fake DHCP server races against the true DHCP server to provide an address from its pool. Once accepted, the victim is now connected and traffic will be passing through the attacker's system.



- **DNS Spoofing :** DNS Spoofing is a type of computer attack wherein a user is forced to navigate to a fake website disguised to look like a real one, with the intention of diverting traffic or stealing credentials of the users. Spoofing attacks can go on for a long period of time without being detected and can cause serious security issues.



Q.4 Write a short note on Risk Analysis.

Ans.: A risk is nothing but intersection of assets, threats and vulnerability.

$A + T + V = R$

So the main components of Risk Assessment are:

- Threats
- Vulnerability
- Impact (i.e. potential loss)
- Likelihood of occurrence (i.e. the probability that an event -- threat successful exploit of a vulnerability – will occur)

Threats is anything that can exploit a vulnerability accidentally or intentionally and destroy or damage an **asset**. Asset can be anything people, property or information. Asset is what we are trying to protect and a threat is what we are trying to protect against. **Vulnerability** means gap or weakness in our protection efforts.

There are 2 methods for Risk Assessment :

1. **Quantitative Risk Assessment :** This methodology is not mostly used by the organizations except for the financial institutions and insurance companies. Quantitative risk is mathematically expressed as Annualised Loss Expectancy (ALE). ALE is the expected monetary loss that can be expected for an asset due to a risk being realised over a one-year period.

   ALE = SLE * ARO

   Single Loss Expectancy (SLE) is the value of a single loss of the asset. This may or may not be the entire asset. This is the impact of the loss. Annualised Rate of Occurrence (ARO) is how often the loss occurs. This is the likelihood.

   Theoretically Quantitative risk assessment seems straightforward but there are issues in assigning values to parameters. While the cost of system is easy to define but indirect costs such as value of information, lost production activity and cost to recover are difficult to define accurately. The other element likelihood is not accurately known.

   Therefore, there is a large margin of error in Quantitative Risk Assessment. Due to unavailability of accurate and complete information it is not cost effective to perform a quantitative risk assessment for a IT System.

2. **Qualitative Risk Assessment :** Qualitative Risk Assessment defines likelihood, impact values and risk in subjective terms, keeping in mind that likelihood and impact values are highly uncertain. Qualitative risk assessments typically give risk results of "High", "Moderate" and "Low". Following are the steps in Qualitative Risk Assessment:

   - **Identifying Threats:** Threats and Threat-Sources must be identified. Threats should include threat-source to ensure accurate estimation. It is important to compile a list of all possible threats that are present across the organization and use this list as the basis for all risk management activities. Some of the examples of threat and threat-source are:
     - Natural Threats : floods, earthquakes etc.
     - Human Threats : virus, worms etc.
     - Environmental Threats – power failure, pollution etc.

   - **identifying Vulnerabilities:** Vulnerabilities are identified by numerous means. Some of the tools are:
     - **Vulnerability Scanners :** This is the software the compare the operating system or code for flaws against the database of flaw signatures.
     - **Penetration Testing :** Human Security analyst will exercise threats against the system including operational vulnerabilities like Social Engineering.

- **Audit of Operational and Management Controls :** Operational and management controls are reviewed by comparing the current documentation to best practices for example ISO 17799 and by comparing actual practices against current documented processes.

- **Relating Threats to Vulnerabilities :** This is the most difficult and mandatory activity in Risk Assessment. T-V pair list is established by reviewing the vulnerability list and pairing a vulnerability with every threat that applies, then by reviewing the threat list and ensuring that all the vulnerabilities that that threat-action/threat can act against have been identified.

- **Defining Likelihood:** Likelihood is the probability that a threat caused by a threat-source will occur against a vulnerability. Sample Likelihood definitions can be like:
  - Low : 0-30% chance of successful exercise of Threat during a one year period
  - Moderate : 31-70% chance of successful exercise of Threat during a one year period
  - High : 71-100% chance of successful exercise of Threat during a one year period

  This is just a sample definitions. Organization can use their own definition like Very Low, Low, Moderate, High, Very High.

- **Defining Impact:** Impact is best defined in terms of impact upon confidentiality, integrity and availability. Sample definitions for impact are as follows:

	Confidentiality	Integrity	Availability
Low	Loss of Confidentiality leads to Limited effect on organization	Loss of Integrity leads to Limited effect on organization	Loss of Availability leads to Limited effect on organization
Medium	Loss of Confidentiality leads to Serious effect on organization	Loss of Integrity leads to Serious effect on organization	Loss of Availability leads to Serious effect on organization
High	Loss of Confidentiality leads to Severe effect on organization	Loss of Integrity leads to Severe effect on organization	Loss of Availability leads to Severe effect on organization

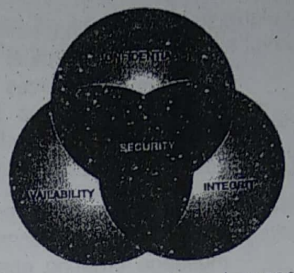
1.3 SECURE DESIGN PRINCIPLES

Q.1 What are the 3 goals of security?

Ans.: CIA focuses on three aspects of information protection that indeed are important, but it is not an all-inclusive model.

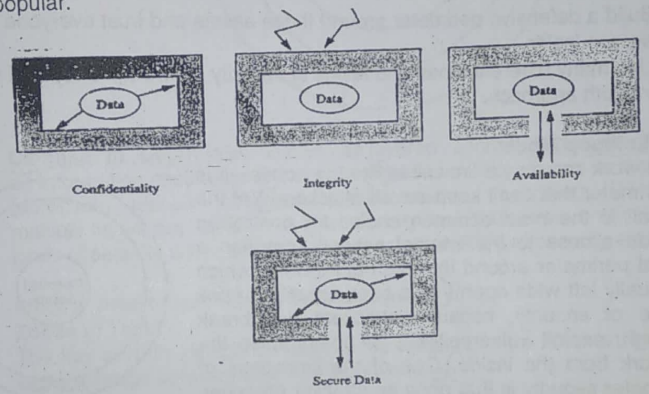
Confidentiality is a set of rules that limits access to information, **integrity** is the assurance that the information is trustworthy and accurate, and **availability** is a guarantee of reliable access to the information by authorized people.

Confidentiality : Confidentiality is the ability to hide information from those people unauthorised to view it. It is perhaps the most obvious aspect of the CIA triad when it comes to security, but correspondingly, it is also the one which is attacked most often. Cryptography and Encryption methods are an example of an attempt to ensure confidentiality of data trasferred from one computer to another.



Integrity : The ability to ensure that data is an accurate and unchanged representation of the original secure information. One type of security attack is to intercept some important data and make changes to it before sending it on to the intended receiver.

Availability : It is important to ensure that the information concerned is readily accessible to the authorised viewer at all times. Some types of security attack attempt to deny access to the appropriate user, either for the sake of inconveniencing them, or because there is some secondary effect. For example, by breaking the web site for a particular search engine, a rival may become more popular.



Data Confidentiality :
Data can be gathered by many means, such as tapping wires, planting bugs in output devices, sifting through trash receptacles, monitoring electromagnetic radiation, bribing key employees, inferring one data point from other values, or simply requesting the data. Because data are often available in a form people can read, the confidentiality of data is a major concern in computer security.

Data Integrity :
Stealing, buying, finding, or hearing data requires no computer sophistication, whereas modifying or making new data requires some understanding of the technology by which the data are transmitted or stored, as well as the format in

which the data are maintained. Thus, a higher level of sophistication is needed to modify existing data or to fabricate new data than to intercept existing data. The most common sources of this kind of problem are malicious programs, errant file system utilities, and flawed communication facilities. Data are especially vulnerable to modification. Small and skillfully done modifications may not be detected in ordinary ways.

A more complicated process is trying to reprocess used data items. With the proliferation of telecommunications among banks, a fabricator might intercept a message ordering one bank to credit a given amount to a certain person's account. The fabricator might try to **replay** that message, causing the receiving bank to credit the account again. The fabricator might also try to modify the message slightly, changing the account to be credited or the amount, and then transmit this revised message.

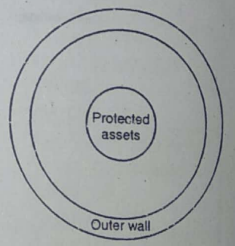
Q.2 What are the different defense models?
OR
Compare lollipop model vs onion model.

Ans.: There are two approaches you can take to preserve the confidentiality, integrity, availability, and authenticity of electronic and physical assets such as the data on your network:

- Build a defensive perimeter around those assets and trust everyone who has access inside.
- Use many different types and levels of security controls in a layered defense-indepth approach.

The Lollipop Model :

In network security, a firewall is like the house—it is a perimeter that can't keep out all attackers. Yet the firewall is the most common choice for controlling outside access to the internal network, creating a virtual perimeter around the internal network (which is usually left wide open). This often creates a false sense of security, because attackers can break through, exploit vulnerabilities, or compromise the network from the inside. One of the limitations of perimeter security is that once an attacker breaches the perimeter defense, the valuables inside are completely exposed.



As with a lollipop, once the hard, crunchy exterior is cracked, the soft, chewy center is exposed. That's why this is not the best model of defense.

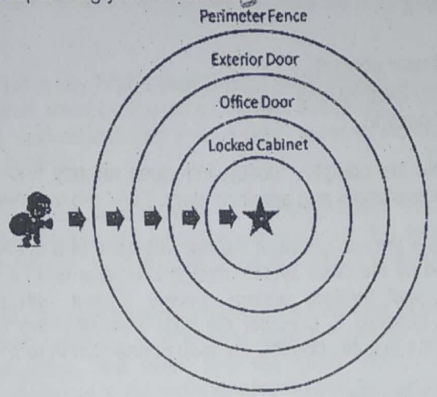
The Onion Model :

A layered security architecture, like an onion, must be peeled away by the attacker, layer by layer, with plenty of crying.

When it comes to protecting a small business network from Ransomware, viruses, malware, improper browsing, etc., you have to have a layered approach to security.

Defense in depth has long been explained by using the onion as an example of the various layers of security. The outer layer contains the firewall. Middle layers contain v.

Anyone who obtains the username and password, or hijacks an account that's already logged in, can gain full access to the system. Since there are no other layers that must be bypassed, the system would be completely compromised. If such a system had further layers of security controls that needed to be passed after the username and password authentication, compromising the system would be correspondingly more difficult.



Defense in Depth (also known as layered security and layered defense) is an information assurance (IA) concept. It uses multiple layers of security controls (defenses) placed throughout an information technology (IT) system. The multiple layers are not of the same security tool. It uses several several different kinds of security with each protecting against a different security attack.

Q.3 What is zone of trust and why it is required?

Ans.: Zones of Trust :

The key security design decision is the balance to be taken at every step of a system design between trust and inconvenience.

For every system to system, subsystem to subsystem and component to component connection a decision must be made as to whether either side of the connection will trust the other, and to what degree. Trust is in some ways analogous to coupling. The higher the level of trust, the more likely that a compromise of one side of the connection will lead to the compromise of the other.

High trust connections can be characterised by being:

- Unauthenticated
- Executed with elevated or system level privileges irrespective of the user context
- Unencrypted or merely obfuscated

Such high trust connections are the common 'out of the box' configurations of many products. They are also significantly less complicated for developers or administrators to implement correctly and so paradoxically are less likely to have implementation security flaws. They are convenient.

As the trust level of a connection drops it requires security controls to be added to manage the increased risk of allowing the connection. These security controls could be:

- Network flow control
- Authentication
- Encryption
- Maintained user context
- Authorisation Permissions
- Content inspection

Security controls are complex, costly, introduce latency and are usually poorly understood by developers and administrators. They are inconvenient.

There is always a tension between the security view of a system design and the other views held by the other system design specialisms. In a perfect world with a well-scoped, well funded, system delivery project with plenty of time to implement it is possible to consider the trust level of every connection and to design appropriate security controls for each connection in turn.

No project is ever like this.
In order to increase my coverage as a security architect I tend to use the following conceptual tools:

- Zones of trust
- Connection patterns
- Choke points

These dramatically reduce the time I need to design and assure systems.
Zones of trust are a defined area of the system whereby by necessity, by the presence of key information assets and by the wider environmental context the connections within the zone are treated as at the same level of trust. This effectively couples the components within that subsystem for security purposes.

Connection patterns outline the requirements for security controls on the connections within each zone of trust. These should aim to be focused more on the requirement (e.g. transport encryption) than the technical solution (e.g. SSL) as there is always more than one way of doing things and product vendors won't always choose the same one you have. These patterns have to consider the environmental context of the zone as a whole. For example are the components within the zone connected by dedicated switching fabric? and are they in a secure physical hosting environment?, if so then transport encryption may well be overkill.

Choke points are the interconnections between the zones of trust. These define the total interaction between different zones of trust and are the focus of my time on security controls. This is where I assure the strength of the security zones.

A key activity is to not only understand the functional flow of the system into and out of the zone of trust but also the non-functional-aspects such as:

- How is the zone managed?
- Where are the patches deployed from?
- Does the zone have dedicated switch fabric?
- Does the zone have dedicated virtual machine hosts?
- Is the zone in a locked rack?

Extensive (And expensive!) functional security designs can be easily subverted by a single administration laptop with access to all the zones of trust in the system.

Zones of trust is a key High-Level Design architectural view. It relies on re-using the logical views used by the other system designers in order to allow them to subsequently understand why I am asking them to inconvenience themselves with security controls.

Sometimes a zoned view is easy to identify through the design or discovery processes. Sometimes you need tools to tease out the subtleties you would not otherwise have seen. I will discuss some of the tools I have used in a future post.

Q.4 What are the different best practices to be followed to secure the system?

Ans.; You must stop malicious mobile code from arriving on the desktop in the first place, close holes, and make sure the users' computers are appropriately configured. There are many countermeasures you can implement to minimize the risk of a successful attack.

- **Secure the Physical Environment :**

Depending on your environment, PCs and laptops might need to be physically secured to their desks. If anyone leaves their laptop on their desk overnight, it should be secured.

- **Password Protect Booting :**

This is especially important for portable computers, such as laptops and tablets and smartphones. Smallform-factor PCs are the most likely candidates to be stolen. Since most portable devices often contain personal or confidential information, password-protecting the boot sequence might keep a nontechnical thief from easily seeing the data on the hard drive or storage RAM. If a boot-up password is reset on a tablet or smartphone, often it requires that the data be erased too, so confidentiality and privacy are assured.

- **Password Protect CMOS :**

The CMOS/BIOS settings of a computer contain many potential security settings, such as boot order, remote wake-up, and antivirus boot-sector protection. It is important to ensure that unauthorized users do not have access to the CMOS/BIOS settings. Most CMOS/BIOSs allow you to set up a password to prevent unauthorized changes. Some boot-up passwords are able to be bypassed by using a special bootable floppy disk.

- **Disable Booting from USB and CD :**

Disabling booting from USB storage devices and optical drives will prevent boot viruses from those devices and stop attackers from bypassing operating system security by loading a different operating system on the computer.

- **Keep Patches Updated :**

Keeping any technology system up-to-date with the latest software is crucial, because vendors find and fix vulnerabilities over time. Don't let a vulnerability hang around on your systems waiting for an attacker to exploit.

- **Use an Antivirus Scanner :**

It should be deployed on your desktop, with forced, automatic updates, and it should be enabled for real-time protection. The AV solution should be enabled for real-time protection so it scans every file as it comes into the system or enters the computer's memory, so it can prevent malware from executing.

Use Firewall Software :

- Secure Network Share Permissions
- **Use Encryption :** To turn on EFS, right-click a file or folder, choose the Properties tab, click the Advanced button under the Attributes section, and then choose Encrypt.Contents to Secure Data. Linux and Unix administrators should be using SSH instead of Telnet or FTP to manage their computers. The latter utilities work in plaintext over the network, whereas SSH is encrypted.

- **Back Up the System :** Worms and viruses often delete files, format hard drives, or intentionally corrupt data. Even malware that does nothing intentionally wrong to a system's files is maliciously modifying a system just by being present. Security experts cannot always repair the damage and put the system back to the way it was prior to the exploit. This means it's important to keep regular, tested backups of your system.

❑❑❑❑❑

Unit III

Secure Network Design, Network Device Security, Firewalls & Wireless Network Security

SYLLABUS **Weightage : 15 Marks**

Secure Network Design : Introduction to Secure Network Design, Performance, Availability, Security.

Network Device Security : Switch and Router Basics, Network Hardening.

Firewalls : Overview, The Evolution of Firewalls, Core Firewall Functions, Additional Firewall Capabilities, Firewall Design.

Wireless Network Security : Radio Frequency Security Basics, Data-Link Layer Wireless Security Features, Flaws, and Threats, Wireless Vulnerabilities and Mitigations, Wireless Network Hardening Practices and Recommendations, Wireless Intrusion Detection and Prevention, Wireless Network Positioning and Secure Gateways.

Topics :

3.1 SECURE NETWORK DESIGN

➢ INTRODUCTION TO SECURE NETWORK DESIGN

Computers and information networks are critical to the success of businesses, both large and small. They connect people, support applications and services, and provide access to the resources that keep the businesses running. To meet the daily requirements of businesses, networks themselves are becoming quite complex.

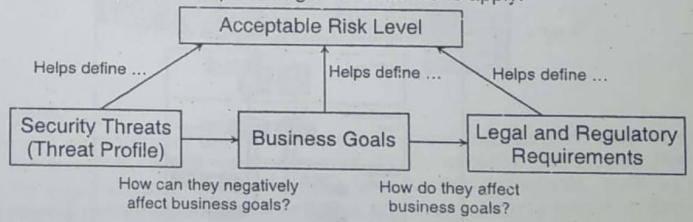
Q.1 What are network requirements for secure design?

Ans.: Most businesses actually have only a few requirements for their network :

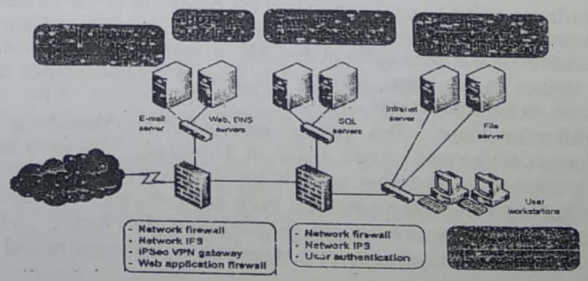
- The network should stay up all the time, even in the event of failed links, equipment failure, and overloaded conditions.
- The network should reliably deliver applications and provide reasonable response times from any host to any host.
- The network should be secure. It should protect the data that is transmitted over it and data stored on the devices that connect to it.
- The network should be easy to modify to adapt to network growth and general business changes.
- Because failures occasionally occur, troubleshooting should be easy. Finding and fixing a problem should not be too time-consuming.

Acceptable Risk :

An organization that is risk averse will ultimately accept lower levels of risk and require more security controls in deployed systems. Management's risk tolerance is expressed through the policies, procedures, and guidelines issued to the staff. During the development of the policies that will guide the design of the systems and networks, management should spend the time and effort necessary to determine if any of these special legal considerations apply.



Designing Security into a Network :



Network safeguards are the first protection barrier of IT system resources against threats originating from outside the network (e.g., intruders, malicious code). The principle network security defenses are firewalls, intrusion detection and prevention systems (IPS/IDS), VPN protections and content inspection systems like anti-virus, anti-malware, anti-spam and URL filtering. These hardware and software solutions complement and support the protection mechanisms associated with the operating systems, databases and applications. Deployment of an effective, scalable security system for medium to large scale networks requires careful, well thought out design based on the organization's risk analysis and sound security principles.

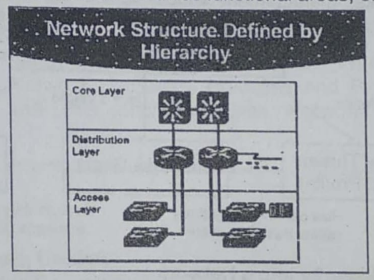
➢ **PERFORMANCE**

The network will play a huge rule in meeting the performance requirements of an organization. Networks are getting faster and faster, evolving from 10 megabit to 100 megabit to gigabit speeds, with 10GE commonly deployed and 40GE, 100GE, and InfiniBand technologies available today. When determining the appropriate network technology, be sure that it can meet the bandwidth requirements projected for three to five years in the future. Otherwise, expensive replacements or upgrades may be required.

The three-tier hierarchy still applies to campus networks, but no longer to data centers.

The Cisco Three-Layered Hierarchical Model :

Cisco has defined a hierarchical model which simplifies the task fo building a reliable, scalable, and less expensive hierarchical internetwork because rather than focusing on packet construction, it focuses on the three functional areas, or layers, of your network :



- **Core layer :** This layer is considered the backbone of the network and includes the high-end switches and high-speed cables such as fiber cables. This layer of the network does not route traffic at the LAN. In addition, no packet manipulation is done by devices in this layer. Rather, this layer is concerned with speed and ensures reliable delivery of packets.
- **Distribution layer :** This layer is also called the Workgroup layer. This layer includes LAND-based routers and layer 3 switches. This layer ensures that packets are properly routed between subnets and VLANs in your enterprise.
- **Access layer :** This layer includes hubs and switches. This layer is also called the desktop layer because it focuses on connecting client nodes, such as workstations to the network. This layer ensures that packets are delivered to end user computers.

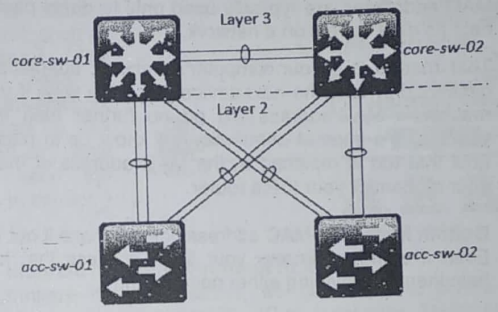
Since the data center network is becoming flatter, faster, and much larger, designing the security components to support the goals of the network is more important than ever.

➢ AVAILABILITY

In information technology, high availability refers to a system or component that is continuously operational for a desirably long length of time. Availability can be measured relative to "100% operational" or "never failing."

Since a computer system or a network consists of many parts in which all parts usually need to be present in order for the whole to be operational, much planning for high availability centers around backup and failover processing and data storage and access. For storage, a redundant array of independent disks (RAID) is one approach. A more recent approach is the storage area network (SAN).

Some availability experts emphasize that, for any system to be highly available, the parts of a system should be well-designed and thoroughly tested before they are used. For example, a new application program that has not been thoroughly tested is likely to become a frequent point-of-breakdown in a production system.



➢ SECURITY

Each element on a network performs different functions and contains data of differing security requirements. Some devices contain highly sensitive information that could damage an organization if disseminated to unauthorized individuals, such as payroll records, internal memorandums, customer lists, and even internal job-costing documents. Other devices have more exposure due to their location on the network. For example, internal file servers will be protected differently than publicly available web servers. When designing and implementing security in network and system architectures, it is helpful to identify critical security controls and understand the consequences of a failure in those controls. For example, firewalls protect hosts by limiting what services users can connect to on a given system. Firewalls can allow different sets of users selective access to different services, such as allowing system administrators to access administrative services while preventing non-administrative users from accessing those same services. This provides an additional level of control over that provided by the administrative mechanisms themselves. By denying a non-administrative user the ability to connect to the administrative service, that user is prevented from mounting an attack directly on that service without first circumventing the firewall.

3.2 NETWORK DEVICE SECURITY

Q.1 Explain different address.

Ans.:

➢ **MAC ADDRESS**

A MAC (or Machine Access Control) address is best thought of as kind of serial number assigned to every network adapter. No two anywhere *should* have the same MAC address. (I'll talk about that "should" more in a moment.)

You can see your network adapter's MAC addresses by using the command prompt in Windows with the **ipconfig /all** command. It looks something like this:

Ethernet adapter Local Area Connection 2:

.

.

Physical Address. . . . . : 00-1D-60-2F-4B-39

Each network adapter on your computer, including wired and wireless interfaces, has one.

MAC addresses are typically used only to direct packets from one device to the next as data travels on a network.

That means that your computer's network adapter's MAC address travels the network only until the next device along the way. If you have a router, then your machine's MAC address will go no further than that. The MAC address of your router's internet connection will show up in packets sent further upstream, until that too is replaced by the MAC address of the next device – likely either your modem or your ISP's router.

Bottom line : your MAC address doesn't make it out very far.
Even if someone knows your MAC address, that knowledge certainly doesn't help them do anything either good or bad.

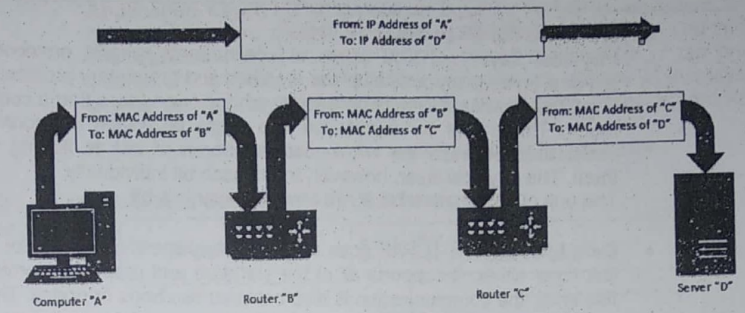
➢ **IP ADDRESS**

An IP address is assigned to every device on a network, so that device can be located on that network.

The internet is just a network, after all – albeit a huge one – and every device connected to it has an IP address. The server that houses *Ask Leo!*, for example, is (currently) at 50.28.23.175. That number is used by the network routing equipment, so when you ask for a page from the site, the request is routed to the right server.

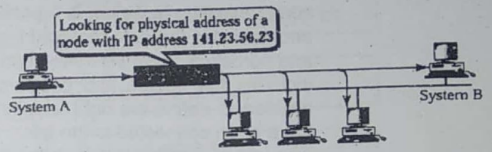
The computers or equipment you have connected to the internet are also assigned IP addresses.

If you're directly connected, your computer will have an IP address that can be reached from anywhere on the internet. If you're behind a router, that router will have the internet-visible IP address, but it will then set up a separate, *private* network to which your computer is connected, assigning IP addresses out of a private range that is not directly visible on the internet. Any internet traffic your computer generates must go through the router, and will appear on the internet to have come from that router.

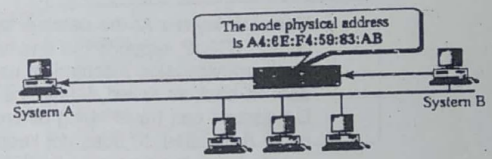


ARP :

Short for Address Resolution Protocol, a network layer protocol used to convert an IP address into a physical address (called a DLC address), such as an Ethernet address. The system will then send a broadcast packet to the network using the ARP protocol to ask "who has 141.23.56.23", only that machine will send the hardware addresses to sender.



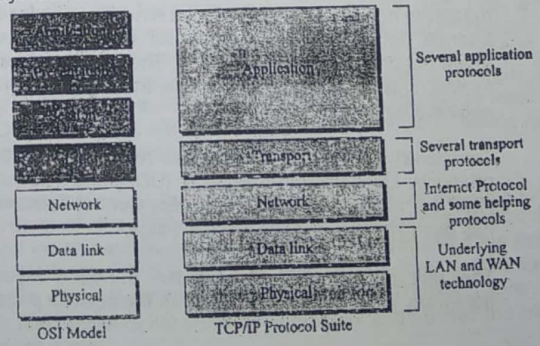
a. ARP request is broadcast



b. ARP reply is unicast

Q.2 Explain the diagram of TCP/IP Protocol Suite.

Ans.: When we compare the two models, we find that two layers, session and presentation, are missing from the TCP/IP protocol suite. These two layers were not added to the TCP/IP protocol suite after the publication of the OSI model. The application layer in the suite is usually considered to be the combination of three layers in the OSI model, as shown in Figure.



Layers in the TCP/IP protocol suite :

- **Physical Layer :** TCP/IP does not define any specific protocol for the physical layer. It supports all of the standard and proprietary protocols. At this level, the communication is between two hops or nodes, either a computer or router. The unit of communication is a single bit. When the connection is established between the two nodes, a stream of bits is flowing between them. The physical layer, however, treats each bit individually.
  The unit of communication at the physical layer is a bit.

- **Data Link Layer :** TCP/IP does not define any specific protocol for the data link layer either. It supports all of the standard and proprietary protocols. At this level, the communication is also between two hops or nodes. The unit of communication however, is a packet called a frame. A frame is a packet that encapsulates the data received from the network layer with an added header and sometimes a trailer. The head, among other communication information, includes the source and destination of frame. The destination address is needed to define the right recipient of the frame because many nodes may have been connected to the link.
  The unit of communication at the data link layer is a frame.

- **Network layer :** At the network layer (or, more accurately, the internetwork layer), TCP/IP supports the Internet Protocol (IP). The Internet Protocol (IP) is the transmission mechanism used by the TCP/IP protocols. IP transports data in packets called datagrams, each of which is transported separately. Datagrams can travel along different routes and can arrive out of sequence or be duplicated. IP does not keep track of the routes and has no facility for reordering datagrams once they arrive at their destination.
  The unit of communication at the network layer is a datagram.

- **Transport Layer :** The network layer is responsible for sending individual datagrams from computer A to computer B; the transport layer is responsible for delivering the whole message, which is called a segment, a user datagram, or a packet, from A to B. A segment may consist of a few or tens of datagrams. The segments need to be broken into datagrams and each datagram has to be delivered to the network layer for transmission. Since the Internet defines a different route for each datagram, the datagrams may arrive out of order and may be lost. The transport layer at computer B needs to wait until all of these datagrams to arrive, assemble them and make a segment out of them.

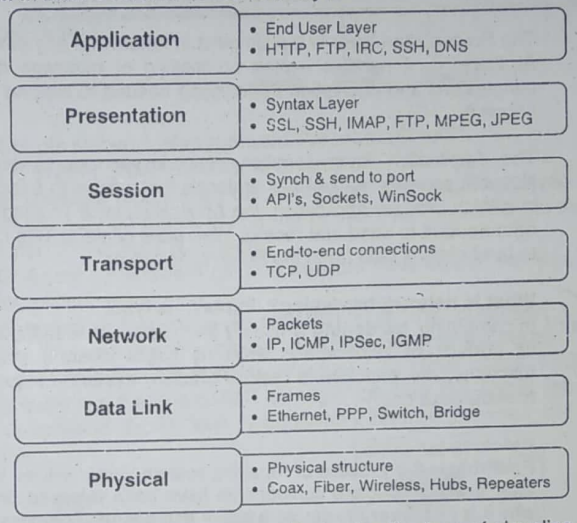
  Traditionally, the transport layer was represented in the TCP/IP suite by two protocols: User Datagram Protocol (UDP) and Transmission Control Protocol (TCP). A new protocol called Stream Control Transmission Protocol (SCTP) has been introduced in the last few years.

  The unit of communication at the transport layer is a segment, user datagram, or a packet, depending on the specific protocol used in this layer.

- **Application Layer :** The application layer in TCP/IP is equivalent to the combined session, presentation, and application layers in the OSI model. The application layer allows a user to access the services of our private internet or the global Internet. Many protocols are defined at this layer to provide services such as electronic mail, file transfer, accessing the World Wide Web, and so on.
  The unit of communication at the application layer is a message.

Q.3 Explain in brief Overview of the OSI Layer.

Ans.:



At the Physical layer, data are transmitted using the type of signaling supported by the physical medium: electric voltages, radio frequencies, or pulses of infrared or ordinary light.

When obtaining data from the Physical layer, the Data Link layer checks for physical transmission errors and packages bits into data "frames". The Data Link layer also manages physical addressing schemes such as MAC addresses for Ethernet networks, controlling access of any various network devices to the physical medium. Because the Data Link layer is the single most complex layer in the OSI model, it is often divided into two parts, the "Media Access Control" sublayer and the "Logical Link Control" sublayer.

The Network layer adds the concept of routing above the Data Link layer. When data arrives at the Network layer, the source and destination addresses contained inside each frame are examined to determine if the data has reached its final destination. If the data has reached the final destination, this Layer 3 formats the data into packets delivered up to the Transport layer. Otherwise, the Network layer updates the destination address and pushes the frame back down to the lower layers.

The Transport Layer delivers data across network connections. TCP is the most common example of a Transport Layer 4 network protocol. Different transport protocols may support a range of optional capabilities including error recovery, flow control, and support for re-transmission.

The Session Layer manages the sequence and flow of events that initiate and tear down network connections. At Layer 5, it is built to support multiple types of connections that can be created dynamically and run over individual networks.

The Presentation layer is the simplest in function of any piece of the OSI model. At Layer 6, it handles syntax processing of message data such as format conversions and encryption / decryption needed to support the Application layer above it.

The Application layer supplies network services to end-user applications. Network services are typically protocols that work with user's data. For example, in a Web browser application, the Application layer protocol HTTP packages the data needed to send and receive Web page content. This Layer 7 provides data to (and obtains data from) the Presentation layer.

Q.4 What is network hardening? Explain its type.

Ans.: In computing, **hardening** is usually the process of securing a system by reducing its surface of vulnerability, which is larger when a system performs more functions; in principle a single-function system is more secure than a multipurpose one.

Patching :

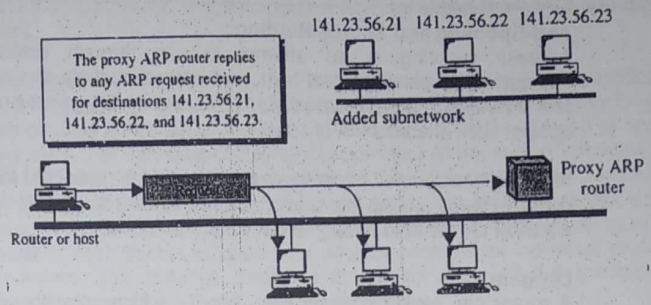
Patching is the process of repairing system vulnerabilities which are discovered after the infrastructure components have been released on the market. This is why it is **necessary** to devise **a patch** management process to ensure the proper preventive measures are taken against potential threats.

Access Control Lists :

An access control list (ACL) is a table that tells a computer operating system which access rights each user has to a particular system object, such as a file directory or individual file. Each object has a security attribute that identifies its access control list. The list has an entry for each system user with access privileges. The most common privileges include the ability to read a file (or all the files in a directory), to write to the file or files, and to execute the file (if it is an executable file, or program).

Proxy ARP :

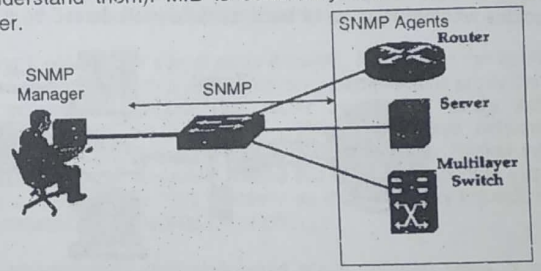
- ARP that acts on behalf of a set of hosts.
- Whenever the router running a proxy ARP receives an ARP request looking for the IP address of one of these hosts, router sends an ARP reply announcing its own hardware (physical) address.
- Later, when the router receives the actual IP packet, it will send the packet to the appropriate host or router.



Q.5 Explain Simple Network Management Protocol (SNMP).

Ans.: Understand SNMP, SNMP consists of 3 items :

- **SNMP Manager** (sometimes called Network Management System – NMS) : a software runs on the device of the network administrator (in most case, a computer) to monitor the network.
- **SNMP Agent :** a software runs on network devices that we want to monitor (router, switch, server...)
- **Management Information Base (MIB) :** is the collection of managed objects. This components makes sure that the data exchange between the manager and the agent remains structured. In other words, MIB contains a set of questions that the SNMP Manager can ask the Agent (and the Agent can understand them). MIB is commonly shared between the Agent and Manager.



For example, in the topology above you want to monitor a router, a server and a Multilayer Switch. You can run SNMP Agent on all of them. Then on a PC you install a SNMP Manager software to receive monitoring information. SNMP is the protocol running between the Manager and Agent, SNMP communication between Manager and Agent takes place in form of messages. The monitoring process must be done via a MIB which is a standardized database and it contains parameters/objects to describe these networking devices (like IP addresses, interfaces, CPU utilization, ...). Therefore the monitoring process now becomes the process of GET and SET the information from the MIB.

Internet Control Message Protocol (ICMP) :

The Internet Control Message Protocol (ICMP) provides a mechanism for reporting TCP/IP communication problems, as well as utilities for testing IP layer connectivity.

Anti-Spoofing and Source Routing :
Address spoofing is an attempt to slip through external defenses by masquerading as an internal host, and internal packets should obviously not be arriving inbound on border routers. Dropping such packets protects the network against such attacks.

In addition to spoofed packets, routers should be configured to drop packets that contain source routing information. Source routing is used to dictate the path that a packet should take through a network.

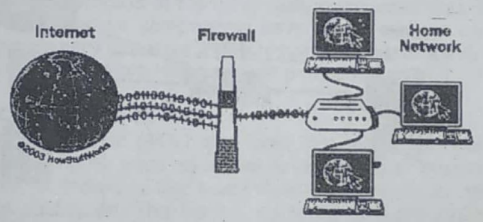
Logging :
A router can export network flow records, which normally need processing to extract useful information, to a collector system. They can also keep records of packets matching access control lists. Whilst continuous logging of all traffic is recommended, often a specific access control list can be useful in answering a question. For instance, it would be possible to log all attempts to send e-mail directly from client computers, in support of a policy that they should not do so.

Where a **VPN (Virtual Private Network)** is implemented in a router or firewall, the device can capture records of use, attempted use and authentication.

3.3 FIREWALLS

➢ OVERVIEW

A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.



Nir Zuk says he developed the technology used in all firewalls today. David Pensak claims to have built the first commercially successful firewall. Marcus Ranum says his own reputation as inventor of the firewall is "marketing BS," and that David Presotto is the man.

Q.1 Write short note on the evolution of firewalls.

Ans.: Generation 1 firewalls, or stateless packet filtering firewalls, operate on the network layer of the OSI Model. As such, they analyze the content headers of individual packets to assess the IP addresses of the sender and receiver. In addition, they recognize the TCP/UDP ports used by hosts on each end of a connection. Using header information, they hinder traffic that doesn't abide by their ACLs. As an example, Juniper produced a stateless packet filter in the

latest Junos OS, which regulates packet flow according to layer 3 and layer 4 headers.

The next generation of firewalls, or Proxy firewalls, operate on the application layer, or the session layer, depending on the iteration. Generally, proxy firewalls handle packets on behalf of the hosts to determine if data is cleared to enter a trusted zone. For example, circuit-level proxies look at the header information as packet filtering firewalls do, operating on the session layer. Meanwhile, application level proxies function on layer 1 to provide granular access control between various processes. Furthermore, application proxies analyze the payloads of each packet to weed out malicious contents for individual protocols and services. For instance, Entensys developed a firewall that incorporates proxy technology with VNP, IDS, and IPS functions.

Generation 3 firewalls, or stateful firewalls, also track the content of packets to verify the integrity of data transmission. For example, they use state tables to enumerate the data being sent. Afterwards, flag values allow authentic packets to be paired with their appropriate sessions, while spoofed packets are filtered out. These firewalls operate on the session layer to protect against playback attacks and session hijacking. E.g., Cisco released a stateful firewall solution, certified under AEL4 with an integrated IPS.

The fourth generation of firewalls, called dynamic packet filters, guards against incoming traffic by developing ACLs for new sessions. Firewalls using this scheme work on the network layer to enable connections through particular ports. Therefore, not all port ranges must be open or susceptible to attack when a trusted client makes a request to an outbound server. In addition to stateless functionality, the latest Junos OS includes dynamic features.

Generation 5 firewalls, or kernel proxy firewalls, function on the application layer to analyze packets through a virtual network. Like previous proxy firewalls, gen 5 handles information remotely, but faster because it ~~solely~~ relies on the processing power of the kernel. In addition, it invokes network stacks to thoroughly assess packets according to their protocols. Packet information of layers 2,3,4,5,7 are all evaluated, hence the term "deep packet inspection". As an example, Cisco's SCE 2020 functions as a kernel proxy firewall, operating on Solaris hardware and a RedHat Linux OS.

Security administrators were concerned about different types of software that could violate security policies, such as :

- **Peer-to-peer file sharing :** Direct system-to-system communication from an inside workstation to another one on the Internet that could leak confidential documents, or expose the organization to liability from music and movie copyright violations.
- **Browser-based file sharing :** Web sites that provide Internet file storage via a web browser, which allow trusted people inside an organization's network to copy files outside the security administrator's area of control.
- **Web mail :** Mail services with the capability to add file attachments to messages, providing a path to theft and leakage of confidential materials.

- **Internet proxies and circumventors :** Services running on the Internet or on local workstations explicitly designed to bypass security controls like web filtering.
- **Remote access :** Remote administration tools, usually used by system administrators to support internal systems from the Internet, which could be abused by Internet attackers

None of these were easy to control using application-aware firewalls, which could really only block broad categories of applications from functioning, or the Internet addresses they needed to connect to, but never with 100 percent effectiveness. That's where fourth generation firewalls come in. These devices have advanced heuristic application detection and behavior management capabilities.

When Applications Encrypt :
Applications that want to bypass firewalls may encrypt their traffic. This makes the firewall's job more difficult by rendering most of the communication unreadable. Blocking all encrypted traffic isn't really feasible except in highly restricted environments where security is more important than application functionality, and a "permit by exception" policy blocks all encrypted application traffic except for that on a whitelist of allowed, known applications.

Applications that encrypt their network traffic can be controlled by fourth-generation firewalls, although it's easier to permit or deny the entire application than it is to control the specific functions within it.

Must-Have Firewall Features : Today's firewalls are expected to do much more than simply block traffic based on the outward appearance of the traffic.

Application Awareness : The firewall must be able to process and interpret traffic at least from OSI layers three through seven. At layer three, it should be able to filter by IP address; at layer four by port; at layer five by network sessions; at layer six by data type, and, most significantly, at layer seven to properly manage the communications between applications.

Accurate Application Fingerprinting : Correct application identification is necessary to ensure that all applications are properly covered by the firewall policy configuration.

Granular Application Control : File transfer, desktop sharing, voice and video, and in-application games are examples of potentially unwanted features that the firewall should be able to control.

Bandwidth Management (QoS) : If a sporting event is broadcast live via streaming video on a popular web site, your firewall should be able to proactively limit or block access so all those people who want to watch it don't bring down your network.

Q.2 Explain core firewall function.

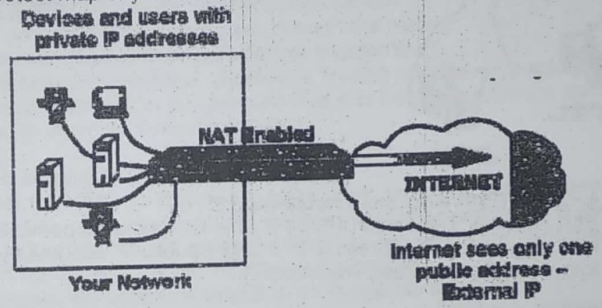
Ans.:

- **Network Address Translation (NAT) :**

Network address translation (NAT) is a technique in which the source and/or destination addresses of IP packets are rewritten as they pass through a router or firewall. It is most commonly used to enable multiple hosts on a private network to connect to the Internet using a single public IP address. NAT is also sometimes referred to as IP masquerading.

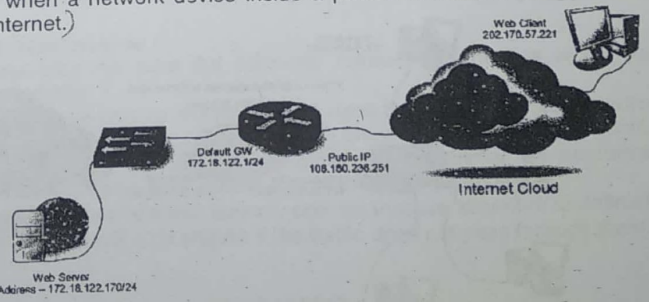
What is Network Address Translation (NAT)?

- Turn one public IP addresses into many.
- Protect map of your network.



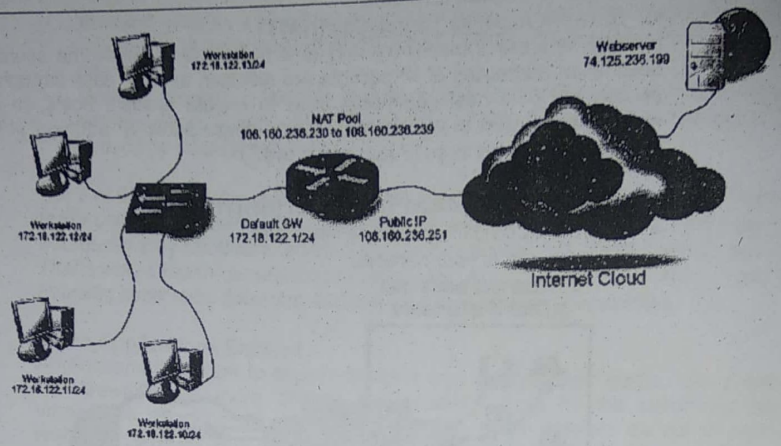
- **Static NAT (Network Address Translation) (SNAT) :**

Static NAT (Network Address Translation) is one-to-one mapping of a private IP address to a public IP address. Static NAT (Network Address Translation) is useful when a network device inside a private network needs to be accessible from internet.



- **Dynamic NAT (Network Address Translation) :**

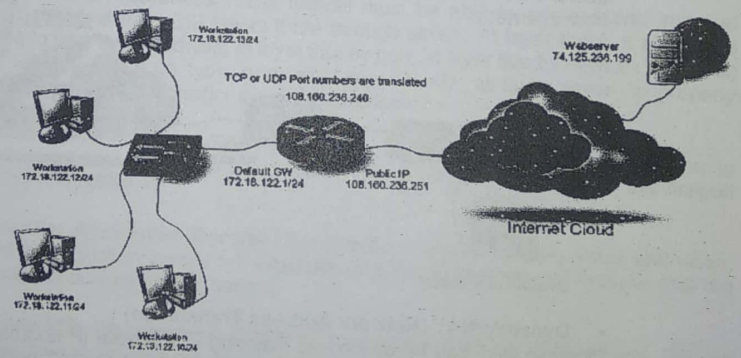
Dynamic NAT can be defined as mapping of a private IP address to a public IP address from a group of public IP addresses called as NAT pool. Dynamic NAT establishes a one-to-one mapping between a private IP address to a public IP address. Here the public IP address is taken from the pool of IP addresses configured on the end NAT router. The public to private mapping may vary based on the available public IP address in NAT pool.



- **PAT (Port Address Translation) :**

Port Address Translation (PAT) is another type of dynamic NAT which can map multiple private IP addresses to a single public IP address by using a technology known as Port Address Translation.

Here when a client from inside network communicate to a host in the internet, the router changes the source port (TCP or UDP) number with another port number. These port mappings are kept in a table. When the router receives from internet, it will refer the table which keep the port mappings and forward the data packet to the original sender.



➢ ADDITIONAL FIREWALL CAPABILITIES

1. Application and Website Malware Execution Blocking
2. Antivirus
3. Intrusion Detection and Intrusion Prevention
4. Web Content (URL) Filtering and Caching
5. E-Mail (Spam) Filtering
6. Enhance Network Performance

Q.3 Explain firewall design.

Ans.: To be effective, firewalls must be placed in the right locations on the network, and configured effectively. Best practices include :

1. All communications must pass through the firewall.
2. The firewall permits only traffic that is authorized.
3. In a failure or overload situation, a firewall must always fail into a "deny" or closed state, under the principle that it is better to interrupt communications than to leave systems unprotected.

Firewall Strengths :

Consider the following firewall strengths when designing network security :

- Firewalls are excellent at enforcing security policies. They should be configured to restrict communications to what management has determined and agreed with the business to be acceptable.
- Firewalls are used to restrict access to specific services.
- Firewalls are transparent on the network—no software is needed on end-user workstations.
- Firewalls can provide auditing. Given plenty of disk space or remote logging capabilities, they can log interesting traffic that passes through them.
- Firewalls can alert appropriate people of specified events.

Firewall Weaknesses :

You must also consider the following firewall weaknesses when designing network security :

- Firewalls are only as effective as the rules they are configured to enforce. An overly permissive rule set will diminish the effectiveness of the firewall.
- Firewalls cannot stop social engineering attacks or an authorized user intentionally using their access for malicious purposes.
- Firewalls cannot enforce security policies that are absent or undefined.
- Firewalls cannot stop attacks if the traffic does not pass through them.

❑❑❑❑❑

Unit IV

Intrusion Detection and Prevention Systems, Voice over IP (VoIP) and PBX Security & Operating System Security Models

SYLLABUS

Weightage : 15 Marks

Intrusion Detection and Prevention Systems : IDS Concepts, IDS Types and Detection Models, IDS Features, IDS Deployment Considerations, Security Information and Event Management (SIEM).

Voice over IP (VoIP) and PBX Security : Background, VoIP Components, VoIP Vulnerabilities and Countermeasures, PBX, TEM : Telecom Expense Management.

Operating System Security Models : Operating System Models, Classic Security Models, Reference Monitor, Trustworthy Computing, International Standards for Operating System Security.

Topics :

4.1 INTRUSION DETECTION AND PREVENTION SYSTEMS

Q.1 Write short note on IDS concepts.

Ans.: An IDS is either a hardware device or software application that uses known intrusion signatures to detect and analyze both inbound and outbound network traffic for abnormal activities.

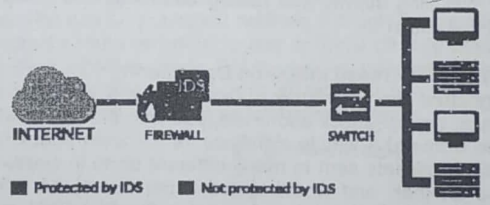
This is done through :

- System file comparisons against malware signatures.
- Scanning processes that detect signs of harmful patterns.
- Monitoring user behavior to detect malicious intent.
- Monitoring system settings and configurations.

Upon detecting a security policy violation, virus or configuration error, an IDS is able to kick an offending user off the network and send an alert to security personnel.

Despite its benefits, including in-depth network traffic analysis and attack detection, an IDS has inherent drawbacks. Because it uses previously known intrusion signatures to locate attacks, newly discovered (i.e., zero-day) threats can remain undetected.

Furthermore, an IDS only detects ongoing attacks, not incoming assaults. To block these, an intrusion prevention system is required.



To be able to fulfill its tasks, IDS must follow certain requirements which are regarded as IDS efficiency evaluation criteria :

- **Accuracy :** IDS must not identify a legal action in a system as an anomaly or a misuse.
- **Performance :** IDS performance must be high enough in to carry out real time intrusion detection.
- **Completeness :** IDS should not ail; to detect an intrusion.
- **Fault Tolerance :** IDS must itself be resistance to attacks and their consequences.
- **Timeliness :** IDS must perform the analysis as quickly as t is possible. It is very important because countermeasures against a detected attack must be accomplished before the attack may damage the system resource or the IDS itself.

Q.2 Explain IDS types and detection model.

Ans.: **Types of IDSs :**

The general types of intrusion detection systems are signature based and heuristic. Signature-based intrusion detection systems perform simple pattern-matching and report situations that match a pattern corresponding to a known attack type.

Heuristic intrusion detection systems, also known as anomaly based builds a model of acceptable behavior and flag exceptions to that model; for the future, the administrator can mark a flagged behavior as acceptable so that the heuristic IDS will treat that previously unclassified behavior as acceptable.

Intrusion detection devices can be network based or host based.
A network-based IDS is a stand-alone device attached to the network to monitor traffic throughout that network.

A host-based IDS runs on a single workstation or client or host, to protect that one host.

Early intrusion detection systems worked after the fact, by reviewing logs of system activity to spot potential misuses that had occurred. The administrator could review the results of the IDS to find and fix weaknesses in the system. Now, however, intrusion detection systems operate in real time (or near real time), watching activity and raising alarms in time for the administrator to take protective action.

- **Signature-Based Intrusion Detection :**

In Signature Based Intrusion Detection, the signature pattern is stored for a particular type of attack and is mapped with the attack when encountered to give related warning. A simple signature for a known attack type might be a series of TCP SYN packets sent to many different ports in succession and at times close to one another, and would cause a port scan. An intrusion detection system would probably find nothing unusual in the first SYN, say, to port 80, and then another (from the same source address) to port 25. But as more and more ports receive SYN packets, especially ports that are not open, this pattern reflects a possible port scan.

The problem with signature–based detection is the signatures themselves. An attacker will try to modify a basic attack in such a way that it will not match the known signature of that attack.

The attacker may insert malformed packets that the IDS will see, to intentionally cause a pattern mismatch; the protocol handler stack will discard the packets because of the malformation. Each of these variations could be detected by IDS, but more signatures require additional work for the IDS, which reduce performance.

Signature–based IDSs cannot detect a new attack for which a signature is not yet installed in the database. Every attack starts, as a new attack at some time, and the IDS is helpless to warm of its existence.

- **Heuristic Intrusion Detection :**

Signatures are limited to specific, known attack patterns; another form of intrusion detection is called heuristic intrusion detection that looks for uncommon behavior. For example, one user might always start the day by reading e–mail, write many documents using a word processor, and occasionally back up files. These action would be normal. This user does not seem to use many administrator utilities. If that person tries to access sensitive system management utilities, this new behavior gives a clue that someone else was acting under the user's identity.

All heuristic instruction detection activity is classified in one of three categories good/benign, suspicious, or unknown. Over time, specific kinds of actions can move from one of these categories to another, depending on the IDS's learning whether certain actions are acceptable or not.

With pattern–matching, heuristic instruction detection is limited by the amount of information the system has seen and how well the current actions fit into one of these categories.

- **Stealth Mode :**

An IDS is a network device and is itself potentially vulnerable to network attacks causing denial of service. To counter these problems, most IDSs run in stealth mode, where and IDS has two network interfaces; one for the network (or network segment) being mentioned and the other to generate alerts and perhaps other administrative needs. The IDS uses the mentioned interface as input only; it never sends packets out through that interface. The interface is configured so that the device has no published address through the monitored interface, that is a router cannot route anything to that address directly because the router does not know such a device exists. It is the perfect passive wiretap. If the IDS need to generate an alert, it uses only the alarm interface on a completely separate control network. Such architecture is shown in Figure.

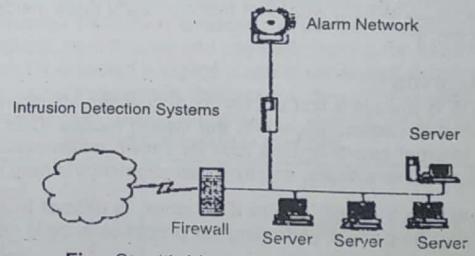


Fig.: Stealth Mode Connected in Two Network.

Q.3 What are IDS features?

Ans.: • **Goals for Intrusion Detection Systems :**

IDS should be fast, simple, and accurate, while at the same time it should be complete. It should detect all attacks with little performance penalty.

- The designs approaches, the IDS can use are as follows:
  - filter on product headers.
  - filter on packet content
  - maintain connection state

- use complex, multipacket signatures
- use minimal number of signatures with maximum effect
- filter in real time, online.
- hide its presence
- use optimal sliding time window size to match signatures.

- **False Results :**

In IDS might detect an intruder correctly most of the time, it may stumble in two different ways; by raising an alarm for something that is not really an attack , or not raising an alarm for a real attack. Many false positives will make the administrator less confident of the IDS's warming's, perhaps leading to a real alarm's being ignored. But false negatives also mean that real attacks are passing the IDS without action. The degree of false positives and false negatives represents the sensitivity of the system. Most IDS implementations allow the administrator to tune the system's sensitivity, to strike an acceptable balance between false positives and negatives.

Q.4 Discuss IDS Strengths and Limitations.

Ans.: Intrusion detection systems are evolving products. However, IDS mechanism continues to change as new research influences the design of products.

Strength of IDS :

IDSs detect an ever-growing number of serious problems. And as we learn more about problems, we can add their signatures to the IDS model. Thus, over time, IDSs continue to improve. At the same time, they are becoming cheaper and easier to administer. IDSs are excellent additions to a network's security. Firewalls block traffic to particular ports or address; they also constrain certain protocols to limit their impact. Firewalls have to allow some traffic to center a protected area. Watching what that traffic actually does inside the protected area is an IDS's job.

Limitations of IDS :

Avoiding IDS is always a first priority for successful attackers. An IDS that is not well defended is useless. However the stealth modes IDSs are difficult even to find on an internal network. IDSs look for known weaknesses. Similar IDSs may have identical vulnerabilities, and their selection criteria may miss similar attacks.

Sensitivity is also the limitation of IDS, which is difficult to measure and adjust. IDSs will never be perfect, so finding the proper balance is critical.

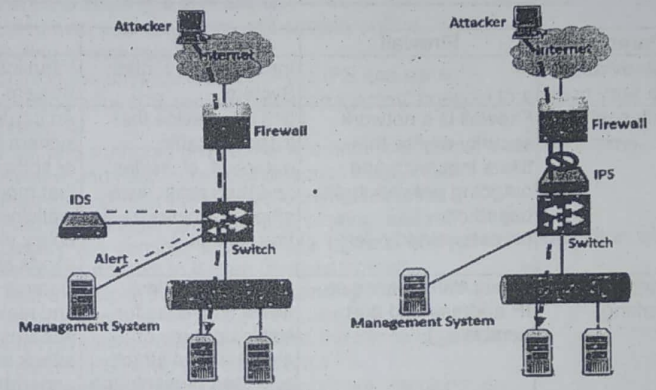
A final limitations is not of IDSs per se, but is one of their uses. An IDS does not run itself, someone has to monitor its track record and respond to its alarms.

Q.5 What is an intrusion prevention system (IPS)?

Ans.: An **Intrusion Detection System (IDS)** is a device or software application that monitors a network or systems for malicious activity or policy violations. Whereas an **Intrusion Prevention System** (IPS) is a network security/threat prevention technology that examines network traffic flows to detect and prevent vulnerability exploits. By blocking the attack rather than just detecting it, Intrusion Prevention allows an organization to shift from a reactive to a proactive security stance. IPS

usually sits behind the firewall and provides a complementary layer of analysis that negatively selects for dangerous content. IPS is placed **inline** (as shown in the above image) on the network i.e. in the direct communication path between source and destination, actively analyzing and taking automated actions on all traffic flows that enter the network. Unlike IDS which only detects the intrusion, IPS not only detects the Intrusion but also take actions on that like Sending an alarm to the administrator, Dropping the malicious packets, blocking traffic from the source address, Resetting the connection etc.

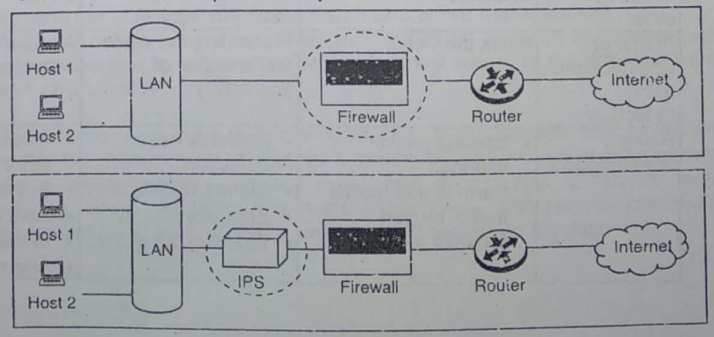
Intrusion Detection System **Intrusion Prevention System**

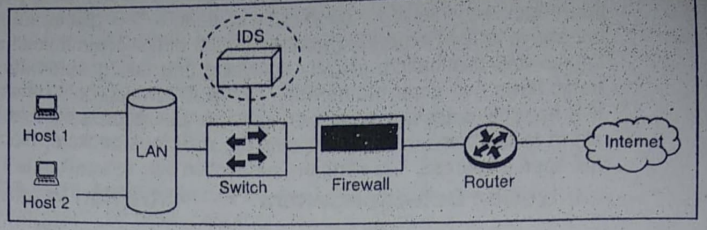


Q.6 Discuss Firewall vs IDS vs IPS.

Ans.:

- **Firewall :** A device or application that analyzes packet headers and enforces policy based on protocol type, source address, destination address, source port, and/or destination port. Packets that do not match policy are rejected.
- **Intrusion Detection System :** A device or application that analyzes whole packets, both header and payload, looking for known events. When a known event is detected a log message is generated detailing the event.
- **Intrusion Prevention System :** A device or application that analyzes whole packets, both header and payload, looking for known events. When a known event is detected the packet is rejected.





Parameter	Firewall	IPS	IDS
Abbreviation for	—	Intrusion Prevention System	Intrusion Detection System
Philosophy	Firewall is a network security device that filters incoming and outgoing network traffic based on predetermined rules.	IPS is a device that inspects traffic, detects it, classifies and then proactively stops malicious traffic from attack.	An intrusion detection system (IDS) is a device or software application that monitors a traffic for malicious activity or policy violations and sends alert on detection.
Principle of working	Filters traffic based on IP address and port numbers.	Inspects real time traffic and looks for traffic patterns or signatures of attack and then prevents the attacks on detection.	Detects real time traffic and looks for traffic patterns or signatures of attack and then generates alerts.
Configuration mode	Layer 3 mode or transparent mode.	Inline mode, generally being in layer 2.	Inline or as end host (via span) for monitoring and detection.
Placement	Inline at the Perimeter of Network.	Inline generally alter firewall.	Non–Inline through port span (or via tap).
Traffic patterns	Not analyzed	Analyzed	Analyzed
Placement wrt each other	Should be 1st Line of defense.	Should be placed after the Firewall device in network.	Should be placed after firewall.
Action on unauthorized traffic detection	Block the traffic	Preventing the traffic on Detection of anomaly.	Alerts/alarms on detection of anomaly.
Related terminologies	• Stateful packet filtering. • Permits and blocks traffic by port/ protocol rules	• Anomaly based detection. • Signature detection • Zero day attacks. • Blocking the attack.	• Anomaly based detection • Signature detection • Zero day attacks • Monitoring • Alarm

➢ IDS DEPLOYMENT CONSIDERATIONS

IDSs are beneficial tools, but they have weaknesses. They need to be fine-tuned if you want to maximize their usefulness, and if you intend to deploy one, you'll need to come up with a deployment plan to do so successfully.

- Increasing Inspection Speed
- Decreasing False Positives
- Using Efficient Logging and Alerting

Q.7 Explain IPS Deployment Plan.

Ans.: Here are the steps to a successful.

1. Document your environment's security policy.
2. Define human roles.
3. Decide the physical location of the IPS and sensors.
4. Configure the IPS sensors and management console to support your security policy.
5. Plan and configure device management (including the update policy).
6. Review and customize your detection mechanisms.
7. Plan and configure any prevention mechanisms.
8. Plan and configure your logging, alerting, and reporting.
9. Deploy the sensors and console (do not encrypt communication between sensors and links to lessen troubleshooting).
10. Test the deployment using IPS testing tools (initially use very broad rules to make sure the sensors are working).
11. Encrypt communications between the sensors and console.
12. Test the IPS setup with actual rules.
13. Analyze the results and troubleshoot any deficiencies.
14. Fine-tune the sensors, console, logging, alerting, and reporting.
15. Implement the IPS system in the live environment in monitor-only mode.
16. Validate alerts generated from the IPS.
17. One at a time, set blocking rules for known reliable alerts that are important in your environment.
18. Continue adding blocking rules over time as your confidence in each rule increases.
19. Define continuing education plans for the IPS administrator.
20. Repeat these steps as necessary over the life of the IPS.

Q.8 Write short note on security information and event management.

Ans.: Security Information and Event Management (SIEM) software gives enterprise security professionals both insight into and a track record of the activities within their IT environment.

SIEM technology has been in existence for more than a decade, initially evolving from the log management discipline. It combined security event management (SEM) – which analyzes log and event data in real time to provide threat monitoring, event correlation and incident response – with security information management (SIM) which collects, analyzes and reports on log data.

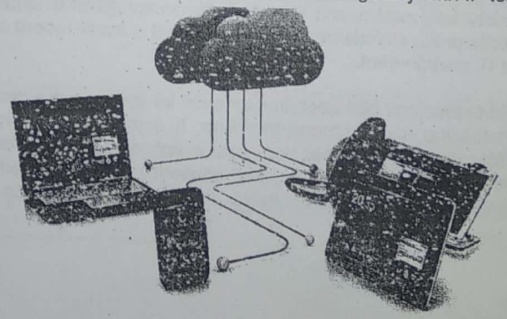
Components :

- **Data aggregation :** Log management aggregates data from many sources, including network, security, servers, databases, applications, providing the ability to consolidate monitored data to help avoid missing crucial events.
- **Correlation :** Looks for common attributes, and links events together into meaningful bundles. This technology provides the ability to perform a variety of correlation techniques to integrate different sources, in order to turn data into useful information. Correlation is typically a function of the Security Event Management portion of a full SIEM solution.
- **Alerting :** The automated analysis of correlated events and production of alerts, to notify recipients of immediate issues. Alerting can be to a dashboard, or sent via third party channels such as email.
- **Dashboards :** Tools can take event data and turn it into informational charts to assist in seeing patterns, or identifying activity that is not forming a standard pattern.
- **Compliance :** Applications can be employed to automate the gathering of compliance data, producing reports that adapt to existing security, governance and auditing processes.
- **Retention :** Employing long-term storage of historical data to facilitate correlation of data over time, and to provide the retention necessary for compliance requirements. Long term log data retention is critical in forensic investigations as it is unlikely that discovery of a network breach will be at the time of the breach occurring.
- **Forensic analysis :** The ability to search across logs on different nodes and time periods based on specific criteria. This mitigates having to aggregate log information in your head or having to search through thousands and thousands of logs.

4.2 VOICE OVER IP (VOIP) AND PBX SECURITY

➢ BACKGROUND

VoIP (voice over IP) is the transmission of voice and multimedia content over Internet Protocol (IP) networks. VoIP historically referred to using IP to connect private branch exchanges (PBXs), but the term is now used interchangeably with IP telephony.



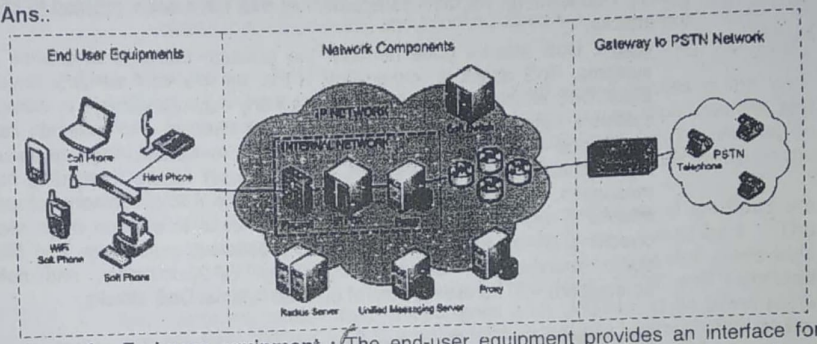
Q.1 How does VoIP work?

Ans.: VoIP uses codecs to encapsulate audio into data packets, transmit the packets across an IP network and unencapsulate the packets back into audio at the other end of the connection. By eliminating the use of circuit-switched networks for voice, VoIP reduces network infrastructure costs, enables providers to deliver voice services over their broadband and private networks, and allows enterprises to operate a single voice and data network.

VoIP also piggybacks on the resiliency of IP-based networks by enabling fast failover following outages and redundant communications between endpoints and networks.

Q.2 What are VOIP components?

Ans.:



1. **End-user equipment :** The end-user equipment provides an interface for users to communicate with other end users. Equipment could be "hard phones" with an interface similar to a conventional telephone or a "soft phone," software that emulates a telephone. The security of such end-user components depends upon how they are installed. Mostly, this end-user equipment often deployed in campus networks, at home, or in hotels. Rarely, however, does the equipment have security features built-in, making them vulnerable to exploitable flaws.

2. **Network components :** VoIP normally uses the existing IP network and thus inherits its vulnerabilities. Each network component has its own security concerns which have surfaced over the past few years (e.g. Goodin, 2008; Chou, 2007). Adding voice traffic to these components increases their list of vulnerabilities. The IP network components, including routers, switches, and firewalls, must also be VoIP-aware to provide security features specified to VoIP. 3. VoIP gateways: Gateway plays an important role in integrating the IP network with the PSTN and thus, care should be taken to ensure that its security policies do not introduce vulnerabilities. The primary functions of a VoIP gateway include voice compression or depression, signaling control, call routing, and packetization. VoIP gateways interface with external controllers such as SIP proxies, H434 Gatekeepers, Media Gateway Controllers (MGC), network management systems, and billing systems. These interfaces can be a

potential weakness because malicious attackers can exploit them to make free telephone calls. Any security framework must counter these attacks quickly and efficiently.

Q.3 Explain VOIP vulnerabilities and countermeasures.

Ans.: VoIP Attacks and Solutions Attackers typically target the most popular and well-publicized systems and applications. VoIP has become one of such application. Several VoIP weaknesses have been revealed recently, thus protocol designers need to address it before successfully deploying VoIP on the global scale. In this section, we present a study of attacks on the VoIP infrastructure. We classify the attacks into five primary types, including: Denial of service (DoS), Eavesdropping, Masquerading, Toll Fraud, and Spam over Internet Telephony (SPIT). Furthermore, we discuss approaches that have been adopted to counter the attacks.

- **DoS :** DoS attacks pose perhaps the greatest threat to enterprise VoIP systems. DoS attack is ranked first in the top five VoIP security threats of 2008. DoS attacks can be directly toward any network element to disrupt the system's functionality or (i) Monitoring and filtering – to maintain lists of suspicious users and deny those users from establishing sessions. (ii) Authentication – to verify the identity of a user before forwarding his/her messages. (iii) Stateless proxy – to reduce the risk of memory exhaustion attacks (DoS) thus stateless proxy can be used to perform other security checks such as authenticating users, registering third party, and filtering spam sources. (iv) Server design (e.g. CPU, memory, and network connection) – to be the first line of defense against DoS attacks.

- **Eavesdropping :** Eavesdropping is the attempt to collect sensitive information to prepare for an attack or gain intelligence. In VoIP, this is a scenario where the attacker is able to monitor signaling or media contents exchanged between users in order to analyze communications to prepare for other future attacks.
  - **Eavesdropping Attacks Reported :** The Internet Security Systems' X-Force team discovered VoIP security flaws in a vender's call manager that would give an attacker the ability to eavesdrop or redirect calls, in addition to gaining unauthorized access to networks running the VoIP products (VoIP Magazine Editorial Staff, 2005). If attackers exploited the vulnerabilities, they could set off a heap overflow within the call manager, causing a DoS condition, and compromising the call manager.
  - **Proposed Solutions for Eavesdropping :** Attacks recommends four strategies to prevent eavesdropping: (i) Employing flawless hardware. (ii)Ensuring that access to wiring closets is restricted to authorized personnel only. (iii) Implementing port based MAC address security on any vulnerable network point; for example, on a reception courtesy phone. (iv) Initiating a procedure to regularly scan the network for devices running in promiscuous mode. Another solution is encryption of VoIP traffic, which is a good method for preventing eavesdropping, however it adds additional overhead.

Masquerading : Masquerading is the ability to impersonate a user, device, or service to gain access to a network, service, network element, or information. Masquerading attacks can be used to commit fraud, unauthorized access to sensitive information, and even service disruption. Perhaps the worst case is that the attackers pretends or takes over someone's identity in the service. Manipulating protocols that provide support for VoIP can also be realized as a masquerading attack in VoIP networks.

Masquerading Attacks Reported : There has been a report that a bank and on-line payment service were victims of attacks where the attacker called a credit-card customer and duped the customer into revealing account information by claiming there had been fraudulent activity.

Proposed Solutions for Masquerading Attacks : An effective authentication module combined with encryption would be an effective solution to masquerading and spoofing attacks.

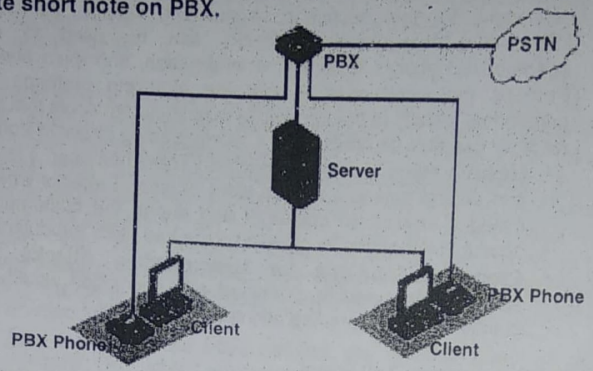
Q.4 Write short note on Toll Fraud.

Ans.: **Toll Fraud :** Toll fraud is the ability to have unauthorized access to the VoIP services for personal or monetary gain. For telecommunication carriers and providers, this is one of the most critical attacks. Toll fraud can be realized by manipulating the signaling messages or the configuration of VoIP components, including the billing systems.

- **Toll Fraud Attacks Reported :** The financial implications of toll fraud are more profound than perceived by telephone subscribers. The Communications Fraud Control Association (CFCA) conducted world-wide survey (Communications Fraud Control Association, 2006) and estimated that telecommunication fraud losses range from US$54.4 to 60 billion (52% increase from 2003's CFCA Survey results). Fraud has been reported as the largest area of revenue leakage for telecommunication operators. According to the Telecomasia.net survey (Chau, 2007), the overall levels of revenue leakage among global telecommunication operators were increased from 12.1% in 2006 to 13.6% in 2007. In recent scam (Blackwell, 2006), a Spokane resident hacked into an unprotected corporate IP network and into the networks of several VoIP providers. Attacker routed traffic from the company's customer through the corporate network to the VoIP providers. The providers were left with the interconnect charges (as much as $300,000 per victim). A Miami service provider was reported to have hacked into other provider networks, routing his customers' calls onto their networks, and then billing his customers (Teal, 2006).
- **Proposed Solutions for Toll Fraud Attacks :** VoIP providers can prevent toll fraud by properly configuring firewalls and by protecting ports. VoIP providers must also actively monitor their networks, so that they know who is accessing the network and with what frequency, and who is generating what kind of traffic.

Q.5 Write short note on PBX.

Ans.:



PBX stands for Private Branch Exchange, which is a private telephone network used within a company or organization. The users of the PBX phone system can communicate internally (within their company) and externally (with the outside world), using different communication channels like Voice over IP, ISDN or analog. A PBX also allows you to have more phones than physical phone lines (PTSN) and allows free calls between users. Additionally, it provides features like transfer calls, voicemail, call recording, interactive voice menus (IVRs) and call queues.

Technological advances in Private Branch Exchange :
Telephone systems have evolved from mechanical devices in the early telephone age to highly complex, digital devices. Due to Voice-over-IP telephony the Private Branch Exchange is evolving more and more into a software-based solution which can be hosted on a local server or at a computer center in the cloud. Cloud-based telephone systems offer maximum flexibility, can be used regardless of location and do not require the company to provide hardware to operate the system.

Hacking a PBX : Attackers hack PBXs for several reasons :

- To gain confidential information (espionage).
- To place outgoing calls that are charged to the organization's account (and thus free to the attacker)
- To cause damages by crashing the PBX.

Securing a PBX : Here is a checklist for securing a PBX :

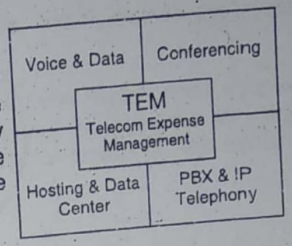
- Connect administrative ports only when necessary.
- Protect remote access with a third-party device or a dial-back.
- Review the password strength of your users' passwords.
- Allow passwords to be different lengths, and require the # symbol to indicate the end of a password, rather than revealing the length of the password.
- Disable all through-dialing features.
- If you require dial through, limit it to a set of predefined needed numbers.
- Block all international calls, or limit the number of users who can initiate them.
- Block international calls to places such as the Caribbean that fraudsters tend to call.

- Train your help desk staff to identify attempted PBX hacks, such as excessive hang-ups, wrong number calls, and locked-out mailboxes.
- Make sure your PBX model is immune to common DoS attacks.

Q.6 Write short note on TEM.

Ans.: TEM (TELECOM EXPENSE MANAGEMENT) :

Telecom Expense Management is defined as merely being "the management of wireless and wireline service and asset expenses," while Technology Expense Management is defined as "the management of technology costs such as software licenses, computer equipment, applications, etc."



A way to manage your wireless, voice, and data environment to reduce risk and cost.

If, for example, an unexpected $100,000 phone bill arrives out of nowhere with calls to countries your users have no reason to call, and through investigation you determine that it was the result of a gateway compromise, you could use the TEM capability to check the rest of the PRI or voice services globally to determine if any of the same suspicious or exploited numbers were being called and to help determine if there are other potentially compromised gateways. You would, of course, also want to do an internal network audit of the services and security on the gateways themselves, as you'll want to plug the holes you know about at the same time that the TEM and audit function is checking for leaks elsewhere for you.

Although phone bills are generally not directly related to the security group's main role, it is the objective of every security group to protect stakeholder interests, and TEM can help a security group detect anomalous behavior and operate more quickly and effectively when they are called in to action for this type of an issue.

4.3 OPERATING SYSTEM SECURITY MODELS

Q.1 Explain different OS models.

Ans.: Operating System Models :

The **trusted computing base** (TCB) of a computer system is the set of all hardware, firmware, and/or software components that are critical to its security, in the sense that bugs or vulnerabilities occurring inside the TCB might jeopardize the security properties of the entire system. By contrast, parts of a computer system outside the TCB must not be able to misbehave in a way that would leak any more privileges than are granted to them in accordance to the security policy.

The careful design and implementation of a system's trusted computing base is paramount to its overall security. Modern operating systems strive to reduce the size of the TCB so that an exhaustive examination of its code base (by means of manual or computer-assisted software audit or program verification) becomes feasible.

Security Perimeter – Isolation or Separation

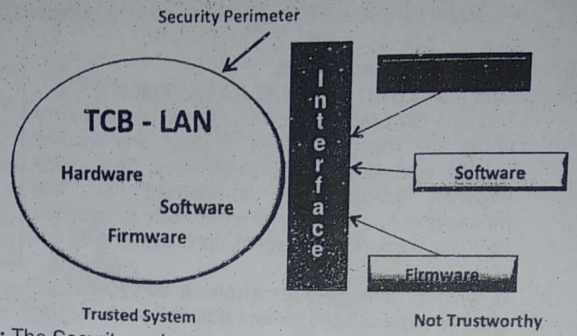


Fig.: The Security perimeter separates the TCB and Non–TCB objects.

Q.2 Discuss the insecurity with underlying protocols.

Ans.: **The Underlying Protocols** are Insecure :

We've known about TCP/IP's lack of security for a long time. The protocol's main problems are as follows :

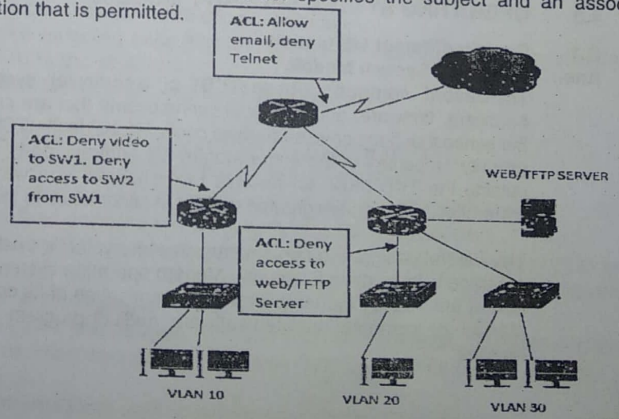
- Vulnerable to spoofing
- Vulnerable to session hijacking
- Predictable sequence guessing
- No authentication or encryption
- Vulnerable to SYN flooding

Q.3 What is ACL and what are the type of ACL?

Ans.: **Access Control Lists :**

Access control list (ACL) refers to the permissions attached to an object that specify which users are granted access to that object and the operations it is allowed to perform.

Each entry in an access control list specifies the subject and an associated operation that is permitted.



Q.4 Differentiate between MAC and DAC.

Ans.:

- **Discretionary Access Control :**

In discretionary access control (DAC), the owner of the object specifies which subjects can access the object. This model is called discretionary because the control of access is based on the discretion of the owner.

Most operating systems such as all Windows, Linux, and Macintosh and most flavors of Unix are based on DAC models.

In these operating systems, when you create a file, you decide what access privileges you want to give to other users; when they access your file, the operating system will make the access control decision based on the access privileges you created.

- **Mandatory Access Control :**

In mandatory access control (MAC), the system (and not the users) specifies which subjects can access specific data objects.

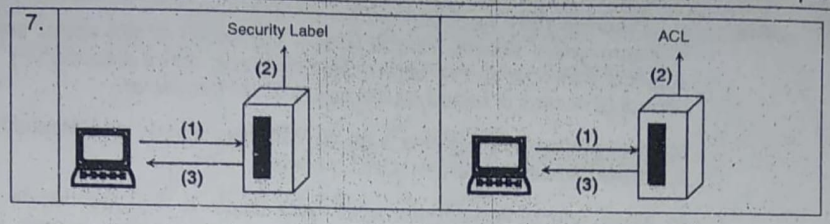
The MAC model is based on security labels. Subjects are given a security clearance (secret, top secret, confidential, etc.), and data objects are given a security classification (secret, top secret, confidential, etc.). The clearance and classification data are stored in the security labels, which are bound to the specific subjects and objects.

When the system is making an access control decision, it tries to match the clearance of the subject with the classification of the object. For example, if a user has a security clearance of secret, and he requests a data object with a security classification of top secret, then the user will be denied access because his clearance is lower than the classification of the object.

The MAC model is usually used in environments where confidentiality is of utmost importance, such as a military institution.

Examples of the MAC-based commercial systems are SE Linux and Trusted Solaris.

	DAC	MAC
1.	A type of access control in which the owner of a resource restricts access to the resource based on the identity of the users.	A type of access control that restricts the access to the resources based on the clearance of the subject.
2.	Stands for Discretionary Access Control.	Stands for Mandatory Access Control.
3.	Resource owner determines who can access and what privileges they have.	Provides access to the users depending on the clearance level of the users. Access is determined by the system.
4.	More Flexible	Less Flexible
5.	Not as secure as MAC.	More Secure
6.	Easier to implement.	Comparatively less easier to implement.



Q.5 Discuss different Classic Security Models.

Ans.: ➢ **Bell-LaPadula**

The **Bell-Lapadula Model** of protection systems deals with the control of *information flow.* It is a linear non-discretionary model. This model of protection consists of the following components:

- A set of *subjects*, a set of *objects*, and an access control matrix.
- Several ordered security levels. Each subject has a clearance and each object has a classification which attaches it to a security level. Each subject also has a current clearance level which does not exceed its clearance level. Thus a subject can only change to a clearance level below its assigned clearance level.

The set of access rights given to a subject are the following:

- **Read-Only**: The subject can only read the object.
- **Append** : The subject can only write to the object but it cannot read.
- **Execute** : The subject can execute the object but can neither read nor write.
- **Read-Write**: The subject has both read and write permissions to the object.

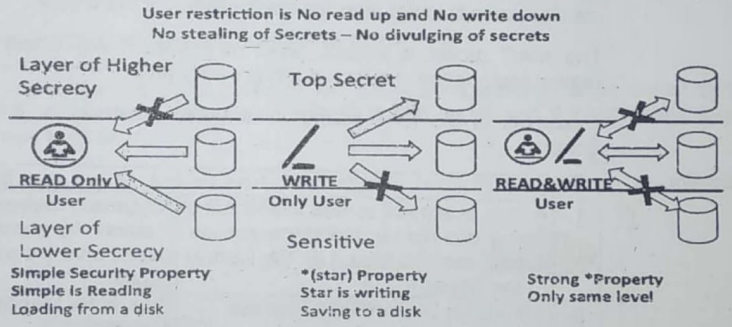


Fig.: Bell–LaPadula Confidentiality Model–Lattice.

➢ **Biba**

Biba is often known as a reversed version of Bell-LaPadula, as it focuses on integrity labels, rather than sensitivity and data classification.

Biba Integrity Model : It addresses integrity of data and uses a lattice of integrity levels. It is also an information flow model like the Bell – Lapadula because they are most concerned about data flowing from one level to another.

The rules of Biba model :

- **Simple integrity rule (no read down) :** it states that a subject cannot read data from a lower integrity level.

SIC U5

Vidyalankar

T.Y. B.Sc. (IT) : Sem. VI

Security in Computing

Unit V : Virtual Machines and Cloud Computing, Secure Application Design & Physical Security

SYLLABUS **Weightage : 15 Marks**

Virtual Machines and Cloud Computing : Virtual Machines, Cloud Computing.

Secure Application Design : Secure Development Lifecycle, Application Security Practices, Web Application Security, Client Application Security, Remote Administration Security.

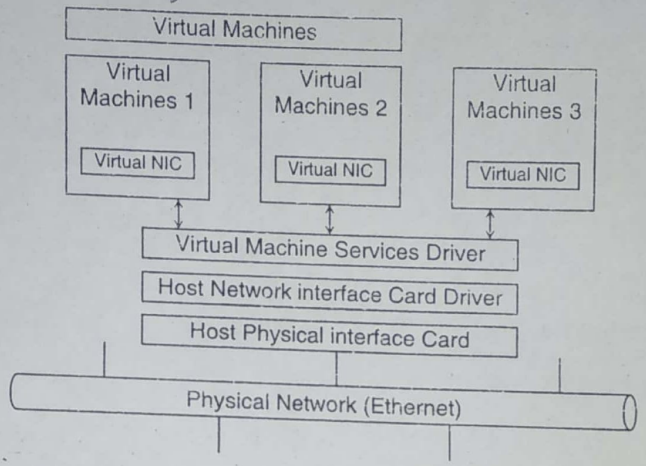
Physical Security : Classification of Assets, Physical Vulnerability Assessment, Choosing Site Location for Security, Securing Assets : Locks and Entry Controls, Physical Intrusion Detection.

Topics :

5.1 VIRTUAL MACHINES AND CLOUD COMPUTING

Q.1 Write short note on Virtual Machines.

Ans.: A virtual machine (VM) is a software program or operating system that not only exhibits the behavior of a separate computer, but is also capable of performing tasks such as running applications and programs like a separate computer. A virtual machine, usually known as a guest is created within another computing environment referred as a "host." Multiple virtual machines can exist within a single host at one time.



Virtual machines are implemented by software emulation methods or hardware virtualization techniques. Depending on their use and level of correspondence to any physical computer, virtual machines can be divided into two categories:

1. **System Virtual Machines :** A system platform that supports the sharing of the host computer's physical resources between multiple virtual machines, each running with its own copy of the operating system. The virtualization technique is provided by a software layer known as a hypervisor, which can run either on bare hardware or on top of an operating system.
2. **Process Virtual Machine :** Designed to provide a platform-independent programming environment that masks the information of the underlying hardware or operating system and allows program execution to take place in the same way on any given platform.

Some of the advantages of a virtual machine include :

- Allows multiple operating system environments on a single physical computer without any intervention.
- Virtual machines are widely available and are easy to manage and maintain.
- Offers application provisioning and disaster recovery options

Some of the drawbacks of virtual machines include :

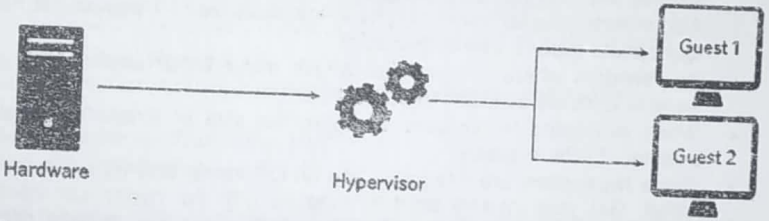
- They are not as efficient as a physical computer because the hardware resources are distributed in an indirect way.
- Multiple VMs running on a single physical machine can deliver unstable performance.

Q.2 What is hypervisor?

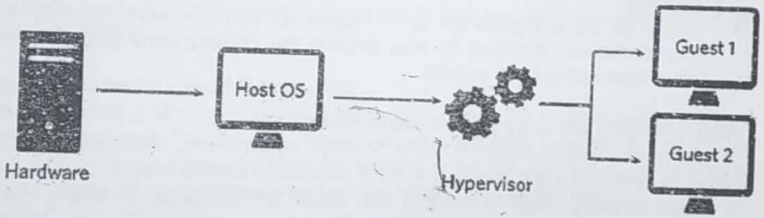
Ans.: A hypervisor is a function which abstracts -- isolates -- operating systems and applications from the underlying computer hardware. This abstraction allows the underlying host machine hardware to independently operate one or more virtual machines as guests, allowing multiple guest VMs to effectively share the system's physical compute resources, such as processor cycles, memory space, network bandwidth and so on. A hypervisor is sometimes also called a virtual machine monitor.

Hypervisor types :

- Type 1 Hypervisor :



- Type 2 Hypervisor :



When a hypervisor is compromised, a hacker can attack each virtual machine (VM) on a virtual host. One possible outcome of a hypervisor attack: The resource usage of a virtual machine can increase, resulting in a denial of service across the host or even a collection of servers. This problem is exacerbated when multiple virtual servers are invoived. But monitoring tools from vendors, such as SolarWinds Inc., VMware, and FlyTrust Inc., can detect and prevent these types of attacks.

Some experts suggest another way to compromise a hypervisor: through the use of rootkits. But it turns out that few people, if anyone, have used this method in the real world. The best-known rootkit is Blue Pill, developed by Rutkowska. This malware executes as a hypervisor to gain control of computer resources. The renegade hypervisor installs without requiring a restart, which makes detection difficult. It can intercept internal communications and send false responses. (Since Blue Pill's release, the Red Pill rootkit was created to detect it.)

Q.3 How to stop hypervisor attack?

Ans.: **Stopping hypervisor attacks before they start :**

In the rush to benefit from virtualization and cloud environments, many users are not seriously considering the security implications. The addition of virtualized

servers, storage and networking in a data center has created new security dependencies that were not found in the physical environments of the past.

If you are just beginning to think about virtualizing your data center, here are some tips for securing your hypervisor to better protect data from the onset:

- Do not view intrusion detection as an option. Nothing is more important than security.
- The hypervisor vendor provides the best intrusion-detection capabilities, because it has the wherewithal to place detection code in the places where intruders are most likely to attack. Get as much information on hypervisor security from the vendor developing or supporting the virtualization platform. Also include your technical experts in this discussion. If you do not have the appropriate experts, hire a consultant.
- Ask vendors where a hypervisor attack might occur and which types of security tools are available to prevent them.
- When evaluating hypervisors, compare the size of attack areas and the number of APIs available.
- Some hypervisors are integrated into an OS kernel and others run on bare metal. Get your internal experts engaged with the hypervisor vendors to discuss why they believe their architecture offers the highest degree of security.
- Study as many hypervisor comparisons as you can, with security in mind. Pay particular attention to who drafted the comparisons and if the reports were sponsored by a vendor.

Implementing security after a deployment :

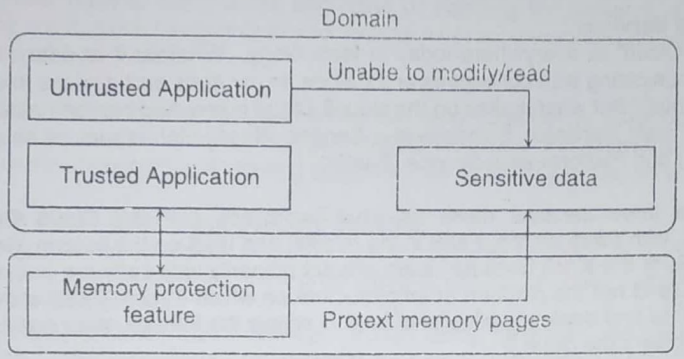
If you have already deployed one or more hypervisors, there are a number of ways to enhance the protection of your virtualized environments:

- Use security tools to monitor the virtual environment, including the virtual servers as well as the network traffic between VMs and hosts. These tools must include oversight and visibility into the virtual administration activities.
- Integrate hypervisor monitoring into your overall system management/ monitoring infrastructure.
- Continuously validate your virtual environment to ensure the integrity and security of your virtual servers.

Q.4 How to protect Guest OS & VPN?

Ans.: Protecting Guest OS :

The main benefit of a virtualization solution is the separation of potentially untrusted guest operating systems from each other and from critical services collocated on the same physical machine, reducing the attack surface and minimizing the possible impact of exploited vulnerabilities. The hypervisor is protected from guest OS actions in such a way that malicious activities by a guest system cannot damage the critical services or the hypervisor itself. An additional benefit of KSH is its ability to reduce expenses on hardware maintenance.



Protecting Virtual Networks :

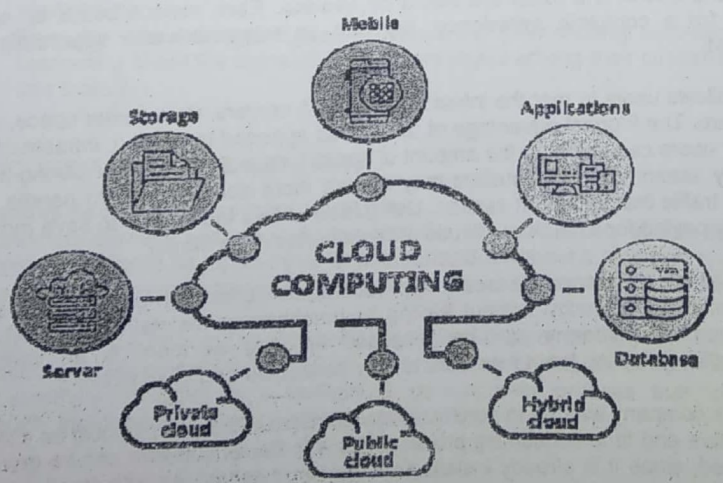
Typically, hypervisors provide three choices for network configurations:

- Network bridging
- Network Address Translation (NAT)
- Host-only networking

Security devices, such as IDSs or IPSs, can monitor and control network traffic using network bridging and NAT and, to a lesser extent, host-only networking. In the case of host-only networking, introspection can be used to compensate for this lack of visibility.

Q.5 Write short note on Cloud Computing.

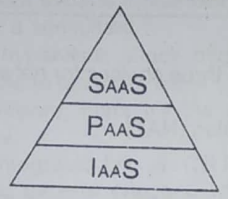
Ans.: Cloud computing is shared pools of configurable computer system resources and higher-level services that can be rapidly provisioned with minimal management effort, often over the Internet. Cloud computing relies on sharing of resources to achieve coherence and economies of scale, similar to a public utility.



Cloud Services :

The "Cloud" is everywhere today in technology. Whether it is data storage, or communicating with colleagues and friends, many apps and devices interact with the cloud. But what makes up the cloud? Cloud computing can be broken up into three main services: Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS).

These three services make up what Rackspace calls the Cloud Computing Stack, with SaaS on top, PaaS in the middle, and IaaS on the bottom. SaaS is on the top of the stack because users interact primarily with software hosted on the cloud, and not the platform or infrastructure on which it runs. PaaS allows users to create and deploy applications. IaaS is simply the infrastructure and hardware that powers the cloud.



The Cloud Stack : SaaS is on top because users primarily interact with software hosted on the cloud, and not the platform or infrastructure on which it runs. PaaS allows users to create and deploy applications. IaaS is the infrastructure and hardware that powers the cloud.

Let us understand the same with the help of transportation example:

The series of roadways and highways represents IaaS, the cars and trucks driving on the roadways represents PaaS, and the goods and people represent SaaS. Without people, the cars and trucks could not go anywhere, and without cars and trucks, the roadways would be useless. Each service builds on each other for a complete experience, but can be interacted with separately as needed.

IaaS allows users to rent the infrastructure itself: servers, data center space, and software. The biggest advantage of renting, as opposed to owning, infrastructure is that users can scale up the amount of space needed at any time. During busy holiday seasons, online retailers may require more server space to handle the heavy traffic than in the off-season. Using IaaS allows the retailer to save money by only paying for what they will use within a certain time frame.

PaaS allows developers to create applications, collaborate on projects, and test application functionality without having to purchase or maintain infrastructure. Development platforms can be accessed as long as there is an internet connection, allowing team members to stay connected and keep working.

When a company wanted to purchase new software in the past, it could be a very expensive and time consuming process. But with SaaS, software can be quickly deployed, since it is already installed on the cloud server. As with PaaS, users only need access to a computer with internet connection to use the software, and

they never have to worry about upgrading or patching the software. SaaS can reduce costs, since users only pay for exactly what is needed and do not have to maintain the software.

Together, these three types of services can work together to save companies time and money in deploying and maintaining hardware and software, and can keep users connected and working collaboratively, even in a global way.

Q.6 Explain Cloud Computing Security Benefits.

Ans.: Cloud computing providers can offer specific security services at a lower cost and with more consistency than organizations can do on their own. Some of these services include :

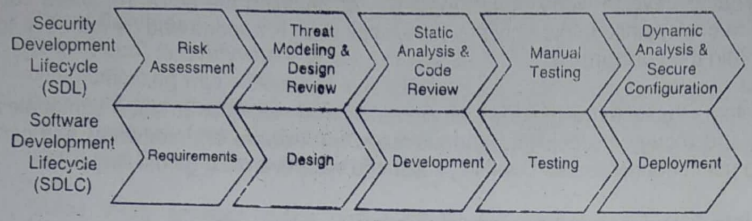
- **Centralized data :** Data leakage through laptop data loss and backup tape loss could conceivably be reduced by cloud computing using thin client technology.
- **Monitoring :** Centralized storage is easier to control and monitor.
- **Forensics and incident response :** With IaaS providers, a dedicated forensic server can be built in the same cloud as the corporate servers but placed offline, ready to be used and brought online as required. It can also reduce evidence acquisition time, allowing immediate analysis of compromised servers. In addition, servers can now be cloned and the cloned disks instantly made available to the Cloud forensics server.
- **Password assurance testing :** For organizations that routinely crack passwords to check for weaknesses, password cracking times can be significantly decreased.
- **Logging :** Effectively unlimited storage for logging, with reduced concerns about insufficient disk space being allocated for system logging.
- **Testing security changes :** Vendor updates and patches, as well as configuration changes for security purposes, can be applied using a cloned copy of the production server, with low-cost impact testing and reduced startup time.
- **Security infrastructure :** SaaS providers that offer security technologies to customers share the costs of those technologies among their customers who use them.

5.2 SECURE APPLICATION DESIGN

Q.1 Discuss Secure Development Lifecycle.

Ans.: Customers demand secure products out of the box, so security should be a top priority that should be top of mind for everyone. But without a standard approach to security, it is almost impossible to deliver on the customers' expectations.

That's where the Secure Development Lifecycle (SDL) comes in.
A secure development lifecycle (SDL, or sometimes SSDL, for secure software development lifecycle) is essentially a development process that includes security practices and decision making inputs.



Finally, because different applications have different security requirements, it is common for an SDL to require all applications to determine their requirements, and then allow applications with lower security requirements to skip some security activities or perform checks less rigorously.

Secure Development Life Cycle (SDL) is a process for developing products that are secure and resilient.

Q.2 Explain Web Application Security.

Ans.: There are several web application security concerns to be considered:

- SQL injection
- Forms and scripts
- Cookies and session management
- General attacks

SQL Injection :

SQL injection is a web security vulnerability that allows an attacker to interfere with the queries that an application makes to its database. It generally allows an attacker to view data that they are not normally able to retrieve. This might include data belonging to other users, or any other data that the application itself is able to access. In many cases, an attacker can modify or delete this data, causing persistent changes to the application's content or behavior.

In some situations, an attacker can escalate an SQL injection attack to compromise the underlying server or other back-end infrastructure, or perform a denial-of-service attack.

Q.3 How does a SQL injection attack work?

Ans.: Imagine a courtroom in which a man named Bob is on trial, and is about to appear before a judge. When filling out paperwork before the trial, Bob writes his name as "Bob is free to go". When the judge reaches his case and reads aloud "Now calling Bob is free to go", the bailiff lets Bob go because the judge said so.

While there are slightly different varieties of SQLi, the core vulnerability is essentially the same: a SQL query field that is supposed to be reserved for a particular type of data, such as a number is instead passed unexpected information, such as a command. The command, when run, escapes beyond the intended confines, allowing for potentially nefarious behavior. A query field is commonly populated from data entered into a form on a webpage.

Let's look at a simple comparison between normal and malicious SQL statements :

- **Normal SQL query :**

In this normal SQL query, the studentId string is passed into a SQL statement. The goal is to look through the list of students for a student that matches the studentId entered. Once found, that student's record will be returned. Put simply, the command says "go find this user and give me their data".

The code might look something like this:

```
studentId = getRequestString("studentId");
lookupStudent = "SELECT * FROM students WHERE studentId = " + studentId
```

If a student enters a student ID of 117 inside a webpage form labelled 'Please enter your student ID number'

Please enter your student ID number : 117

the resulting SQL query will look like:

```
SELECT * FROM students WHERE studentId = 117;
```

This command will return the record for the particular student with a studentId, which is what the developer who wrote the API expects to have happen.

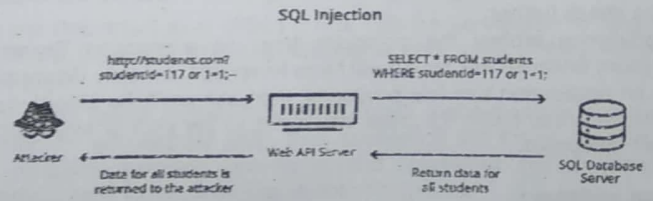
- **SQL Injection query :**

In this example, an attacker instead enters a SQL command or conditional logic into the input field, he enters a student ID number of:

Please enter your student ID number : **117 OR 1=1**

Where normally the query would search the database table for the matching ID, it now looks for an ID or tests to see if 1 is equal to 1. As you might expect, the statement is always true for every student in the column, and as a result, the database will return all data from the students table back to the attacker making the query.

```
SELECT * FROM students WHERE studentId = 117 OR 1=1;
```



Forms and scripts :

Attackers can exploit the data embedded inside forms and can trick the web application into either exposing information about another user or to charge a lower price in e-commerce applications. Three methods of exploiting forms are these:

- Disabling client-side scripts
- Passing parameters in the URLs
- Passing parameters via hidden fields

Cookies and Session Management :

Q.4 Explain Cookies and Session Management.

Ans.: A cookie is a message given to a web browser by a web server. The browser stores the message in a text file. The message is then sent back to the server each time the browser requests a page from the server.

Sessions are used to track user activities, such as a user adding items to their shopping cart—the site keeps track of the items by using the session identifier.

Attackers can abuse both sessions and cookies :

- Session theft
- Managing sessions by sending data to the user
- Web server cookie attacks
- Securing sessions

General Attacks :

Some attacks aren't part of any specific category, but they still pose a significant risk to web applications. Among these are vulnerable scripts, attempts to brute-force logins, and buffer overflows.

Q.5 What is client application security?

Ans.: Application security is mainly controlled by the developer of the application. The administrator can tighten the security for some applications, but if the application is not secure by nature, it's not always possible to secure it.

From the administrator's point of view, there are a number of security issues to keep in mind :

Running privileges :

An administrator should strive to run an application with the fewest privileges possible. Doing so protects the computer against several threats:

- If the application is exploited by attackers, they will have the privileges of the application. If the privileges are low enough, the attackers won't be able to take the attack further.
- Low privileges protect the computer from an embedded Trojan (in the application) because the Trojan will have fewer options at its disposal.
- When an application has low privileges, the user won't be able to save data in sensitive areas (such as areas belonging to the OS) or even access key network resources.

Application updates :

It is always necessary to keep the system up to date and keep all patches updated.

- Manual updates
- Automatic updates
- Semi-automated updates
- Physical updates

Integration with OS security :

When an application is integrated with OS security, it can use the security information of the OS, and even modify it when needed. This is sometimes required by an application, or it may be supplied as an optional feature.

Q.6 Discuss remote administration security.

Ans.: Most of today's applications offer remote administration as part of their features, and it's crucial that it be secure. If an attacker manages to penetrate the administration facilities, other security measures can be compromised or bypassed.

Reasons for Remote Administration :

Remote administration is needed for various reasons :

- **Relocated servers :** Computers that belong to an organization but that are physically located at the ISP.
- **Physical distance :** An administrator may need to manage a large number of computers in the organization. Some organizations span several buildings (or cities), and physically attending the computers can be a tedious and time-consuming task. Additionally, physical access may be limited to the actual data centers.

HTTP Authentication Methods :

Before delving into the problem of remote administration, it's important to go over the current methods available to authenticate HTTP connections:

- **Basic authentication :** When a page requires basic authentication, it replies to the browser with error code 401 (unauthorized) and specifies that basic authentication is required. The browser encodes the username and password using BASE64 encoding and sends it back to the server. If the login is correct, the server returns message number 200, which means everything is OK. If the login fails, it replies with the same 401 error as before.
- **Digest authentication :** Digest authentication uses MD5 to hash the username and password, using a challenge supplied by the web server.
- **Secure Sockets Layer (SSL) :** SSL can be configured to require a client certificate (optional) and authenticate a user only if they have a known certificate.
- **Encrypted basic authentication :** Basic authentication can be used in conjunction with regular SSL, thus encrypting the entire session, including the BASE64 encoded username and password (which is very weak encoding, easy to decode—this is not encryption).
- **CAPTCHA :** This is a popular method of verifying that the person on the other end is a human being, by showing a distorted image of letters and numbers and requiring the user to type them in correctly.

5.3 PHYSICAL SECURITY

Q.1 Define and discuss classification of assets.

Ans.: **Classification of assets** is the process of identifying physical assets and assigning criticality and value to them in order to develop concise controls and procedures that protect them effectively.

In information security, computer security and network security, an asset is any data, device, or other component of the environment that supports information-related activities. Assets generally include hardware (e.g. servers and switches), software (e.g. mission critical applications and support systems) and confidential information. Assets should be protected from illicit access, use, disclosure, alteration, destruction, and/or theft, resulting in loss to the organization

We can broadly classify assets in the following categories:

1. Information assets :

Every piece of information about your organization falls in this category. This information has been collected, classified, organized and stored in various forms.

- **Databases :** Information about your customers, personnel, production, sales, marketing, finances. This information is critical for your business. It's confidentiality, integrity and availability is of utmost importance.
- **Data files :** Transactional data giving up-to-date information about each event.
- **Operational and support procedures :** These have been developed over the years and provide detailed instructions on how to perform various activities.
- **Archived information :** Old information that may be required to be maintained by law.
- **Continuity plans, fallback arrangements :** These would be developed to overcome any disaster and maintain the continuity of business. Absence of these will lead to ad-hoc decisions in a crisis.

2. Software assets :

These can be divided into two categories :

(a) **Application software :** Application software implements business rules of the organization. Creation of application software is a time consuming task. Integrity of application software is very important. Any flaw in the application software could impact the business adversely.

(b) **System software :** An organization would invest in various packaged software programs like operating systems, DBMS, development tools and utilities, software packages, office productivity suites etc.

Most of the software under this category would be available off the shelf, unless the software is obsolete or non-standard.

3. Physical assets :

These are the visible and tangible equipment and could comprise of :

(a) Computer equipment : Mainframe computers, servers, desktops and notebook computers.

(b) Communication equipment : Modems, routers, EPABXs and fax machines.
(c) Storage media : Magnetic tapes, disks, CDs and DATs.
(d) Technical equipment : Power supplies, air conditioners.
(e) Furniture and fixtures

Physical Vulnerability Assessment :
A physical security vulnerability assessment, much like its information security, that relies upon measurements of exposure to an applicable risk.

For example, is that network connection in the reception area or public conference room active? Is Wi-Fi connectivity available for visitors? If so, is it getting an IP address via DHCP? Is it segmented on a VLAN? Is a username and password combination required to log in?

Four main areas should be a part of any physical vulnerability assessment: buildings, computing devices and peripherals, documents, and records and equipment.

Choosing Site Location for Security :
There are many security considerations for choosing a secure site location, a few of which are

- Accessibility
- To the site
- From the site (in the event of evacuation)
- Lighting
- Proximity to other buildings
- Proximity to law enforcement and emergency response
- RF and wireless transmission interception
- Utilities reliability
- For a data center, the loss of power may be overcome through the use of generators, but if the water supply is cut off, the AC units will be unable to cool the servers.
- Construction and excavation (past and present)

Q.2 Explain Securing Assets : Locks and Entry Controls.

Ans.: Locks :
Lock up the device or valuable and make it a point to educate the asset owner on the importance of securing the item.

- **Doors and File Cabinets :**

File cabinets containing sensitive information or valuable equipment should be kept locked when not in use.

- **Laptops :**

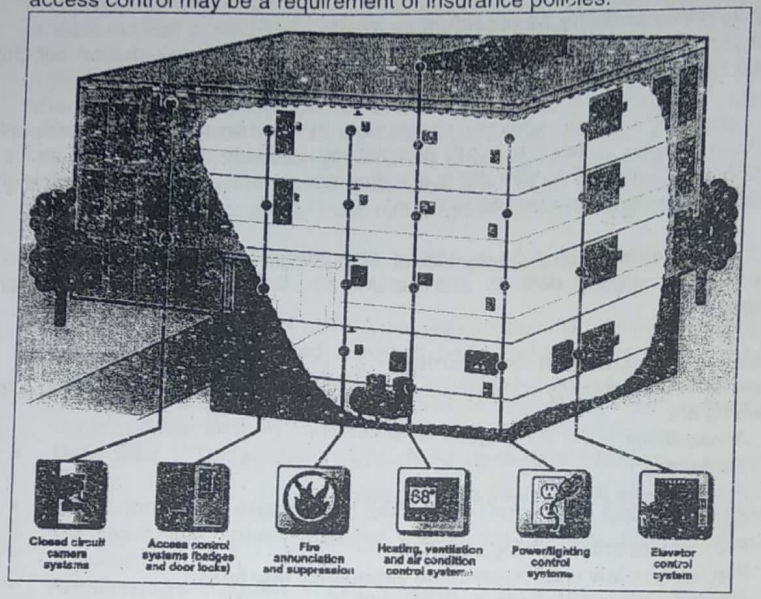
It should be kept highly secured when stationary or while travelling.

- **Data Centers, Wiring Closets, Network Rooms :**

Make sure these rooms are kept locked. If automatic entry-tracking mechanisms are not in use, ensure an access log is kept.

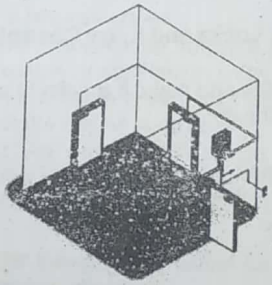
- **Building Access Control Systems :**

Most buildings contain assets that need to be kept safe, secure and protected from theft. Authorised access might be controlled using; doors, gates, turnstiles, secure installations such as safes, barriers, bollards, and so on. Installation of access control may be a requirement of insurance policies.



- **Mantraps :**

Mantraps, which are sometimes called security vestibules, are small rooms with two or more doors. ... On successful authentication, the door to the mantrapun locks automatically, allowing entry to the mantrap. The first door to the mantrap then locks, preventing other individuals from entering the mantrap.

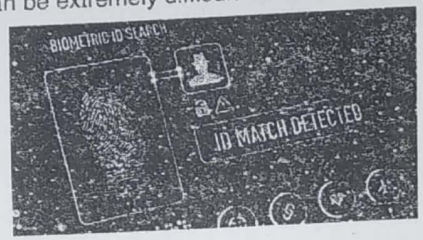


- **Building and Employee IDs :**

Typically, one of the first things any organization does after hiring new employees is to provide them with ID badges. Building and/or employee identification should be displayed at all times, and anyone who lacks a visible ID should be challenged.

- **Biometrics :**

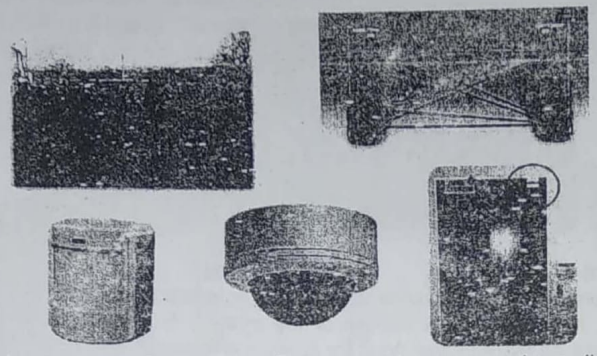
Biometric security devices measure unique characteristics of a person, such as voice pattern, the iris or retina pattern of the eye, or fingerprint patterns. With biometrics, it can be extremely difficult for someone to break into a system.



- **Security Guards :**

A security guard is a person employed by a public or private party to protect the employing party's assets from a variety of hazards by enforcing preventative measures.

Physical Intrusion Detection The fear of unwanted people, breaking into your home and causing harm to your family while sweeping your house clean off its valuables, is a valid one. Intrusion detection systems not only give you security, they also add the element of style to your home with features such as smart lighting control and touch screen controls to adorn your living room. The system is compatible with wireless panic buttons that the elderly can wear and press in case of a medical emergency, or remote viewing of alarms via SMS on your cell phone.



e.g. Perimeter protection ensures that no one jumps over the walls of your home or industry. The IR beam sensors are far more aesthetic as compared to barbwire and have options to ensure the alarm doesn't trigger with cats and birds sitting on the wall.
e.g. Closed-Circuit Television

Ensure that the cabling used for CCTV devices is not readily accessible, so that no one can easily tap into transmissions.

Lighting will also play a critical role in the effectiveness of the camera.
If you are considering the use of a wireless CCTV setup, take into account that anything transmitted through airwaves was also meant to be received, and can be intercepted.

❑❑❑❑❑